HAZMAT TRAINING PAGE 34 | GOOGLE DOCS PAGE 38

CSO
BUSINESS RISK LEADERSHIP

THE GLOBAL STATE OF INFORMATION SECURITY

Our **seventh-annual** survey with PricewaterhouseCoopers finds security leaders struggling to defend new platforms, from **social networking** to **cloud computing**

SEE PAGE 26

www.csoonline.com $9.00 November 2009

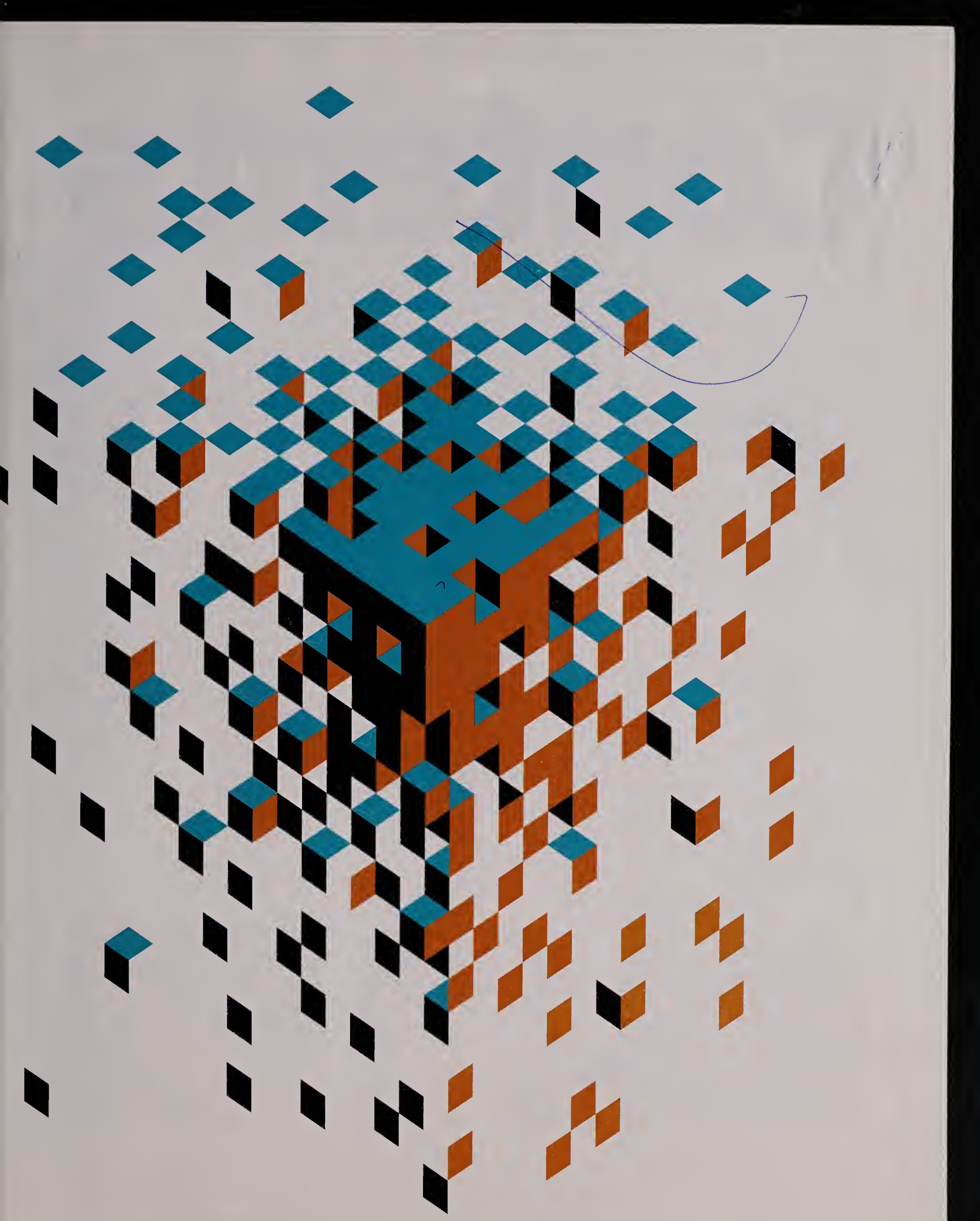
Smarter technology for a Smarter Planet:

Service in the age of smart assets.

Smart assets are making it possible to spread intelligence far beyond the four walls of the datacenter into everything from power lines to railroad lines to assembly lines. The challenge is: how do you choreograph these two worlds—the physical and the digital—to provide the quality services your customers expect and the flexibility your business needs?

IBM's approach to service management can help you extend greater visibility, control and automation through all of your company's services—inside and out—so you can easily modify existing services or quickly add new ones, laying the groundwork for a more dynamic infrastructure. We're helping companies all over the world—20 of the 20 top telcos, 10 of the 20 biggest utilities and 7 of the 10 largest automotive manufacturers—reach beyond the datacenter to deliver quality service and respond quickly to the demands of a smarter planet.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/svcmgmt



IBM, the IBM logo, ibm.com, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Contents

November 2009 Vol.8, No. 9

Features...

26 The Global State of Information Security

Cover Story | Global Security Survey Our seventh-annual survey with PricewaterhouseCoopers finds security leaders struggling to defend new platforms, from social networking to cloud computing. *By Bill Brenner*

34 At the Ready

Crisis Management Chemical giant Dow brings free hazmat-spill education and awareness to emergency responders. *By Joan Goodchild*

Also Inside...

4 **From the Editor**

6 **From the Publisher**

8 **Join the Discussion**
Information Asset Value: Some cold-hearted calculations

13 **Briefing**
- 7 ways security pros DON'T practice what they preach
- A "nightmare" of a Patch Tuesday
- Why pen testing is central to Pennsylvania
- Taking the "closed" out of closed circuit
- 2009 Women of Influence Award winners named
- After attacks, Adobe patches now come faster

22 **Patching Things Up**
Toolbox Software can automate parts of the patch management process—but not all of it. Here's how to choose the right system and get the most from it. *By Mary Brandel*

36 **The Real Problems With Cloud Computing**
Industry View Google may well protect servers better than you do. But your job is to protect information—not just servers. *By Ira Winkler*

38 **Where Defense in Depth Falls Short**
CSO View Hearing about defense in depth can conjure up images of clutter. Ariel Silverstone says he's stumbled upon an example of a better way. *By Ariel Silverstone*

40 **Debriefing**
That's (Not) Hot

CSO (ISSN 1540-904X) is published monthly except for a combined issue in July/August and December/January by CXO Media Inc., 492 Old Connecticut Path, P.O. Box 9208, Framingham, MA 01701-9208. Periodical Postage Rate at Framingham, MA 01701, and at additional mailing offices. Canadian Publications Mail agreement number 1902075. **Canadian Postmaster:** Please return undeliverable copy to P.O. Box 1632, Windsor, ON N9A 7C9. Copyright 2009 by CXO Media Inc. All rights reserved. Reproduction of material appearing in *CSO* is forbidden without written permission. Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by *CSO* for users through the Copyright Clearance Center, provided that a fee of $3.50 per copy of the article is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01970. *www.copyright.com*. Please specify: ISSN 1540-904x. Permission to photocopy does not extend to contributed articles—followed by this symbol: ‡. Address inquiries to *CSO*, P.O. Box 3482, Northbrook, IL 60065; 866 354-1125. *CSO* is free to qualified security executives. To all others the one-year basic rate is $70 for the United States and Canada, $95 to foreign countries (payable in U.S. funds only). The single copy price is $9 to the U.S. and Canada and $15 International. Please allow four to six weeks for new subscriptions to begin. Change of Address: Go to *www.omeda.com/custsrv/cso* and follow the online instructions. **Postmaster:** Send change of address to: *CSO*, P.O. Box 3482, Northbrook, IL 60065. Printed in the USA.

Cover Photo by Veer

4 intellectual properties
0 inquiring minds
Introducing 3M™ Microlouver Technology for your handheld. Mobilize your employees without compromising your data.
3MPrivacyFilters.com/Security
3M™ Mobile Privacy
FOR YOUR EYES ONLY
© 3M 2004. All rights reserved.

Data Junkies

Security surveys—perfect? Of course not. Invaluable? Of course!

Surveys are imperfect. Security metrics are imperfect. No two ways about it.

Lately I've heard two particular complaints down at my favorite online pub, the Blog & Twitter.

One: "You can't calculate the ROI of 'stopping something bad from happening.'"

Two: "Just because a survey shows a practice is common doesn't make it a best practice."

Fair enough. Return on investment is notoriously tricky in evaluating security spending. And there are plenty of Bad Practices that are widely prevalent in the security world; I doubt we need a survey to tell us that.

So we should stop doing surveys? Balderdash.

Handled correctly, survey data does two things for the security field.

One: It helps indicate where and how organizations can improve their security posture.

Two: It helps communicate about security to the rest of the world. Nothing grabs the eye of a busy executive like a key data point.

Starting on Page 26 you'll find Senior Editor Bill Brenner's look at results from the seventh-annual Global State of Information Security survey, conducted as always with PricewaterhouseCoopers and our sister publication *CIO* magazine. This survey is unique in its large, truly global response base—more than 7,000 participants.

If that whets your appetite for more data, we are also working on two other surveys.

1. BSIMM Begin. The Building Security In Maturity Model (BSIMM) is an effort to help companies plan effective software security programs. BSIMM Begin is specifically aimed at companies that are at the very beginning of such a process.

You can participate in the survey at *http://bit.ly/1kZuk*.

2. Data Protection. Together with *CSO*, Forrester is taking a look at how companies protect their data when it's in the hands of business partners or otherwise residing on other assets that the company does not own or directly control.

That survey is fielded at *http://bit.ly/3huACa*.

As we collect and analyze this data, we'll always need to keep our thinking caps on. The more discussion and collaboration we get on surveys and metrics, the better our survey instruments will become. I hope you get a lot out of the PwC data in this issue and will participate in future survey efforts.

-Derek Slater, dslater@cxo.com

Photo by Webb Chappell

CSO

Editor in Chief Derek Slater

Senior Editors

Bill Brenner, Joan Goodchild

Copy Editor

Kristin Burnham

Editorial Administrator

Pat Josefek

Contributors

Mary Brandel, Gregg Keizer, Robert McMillan, Ariel Silverstone, Ira Winkler

DESIGN

Executive Director, Art and Design

Mary Lester

Art Director Steve Traynor

RESEARCH

Research Manager Carolyn Johnson

TECHNICAL ADVISORY BOARD

Jason Cowling

Jeremiah Grossman, WhiteHat Security

Frank Murphy, TBG Security

Stephen Northcutt, SANS Institute

Richard Power, Carnegie Melion CyLab

EDITORIAL/ADVERTISING/ BUSINESS OFFICES

492 Old Connecticut Path,

P.O. Box 9208,

Framingham, MA 01701-9208

Main phone number: 508 872-0080

CXO MEDIA INC.

INTERNATIONAL DATA GROUP

Chairman of the Board

Patrick J. McGovern

IDG COMMUNICATIONS, INC.

CEO Bob Carrigan

Chief Content Officer

John Gallant

BPA WORLDWIDE™

60% OF PRODUCTION VIRTUAL MACHINES ARE LESS SECURE THAN THEIR PHYSICAL COUNTERPARTS.*

THINK CONVENTIONAL SECURITY CAN PROTECT YOUR VIRTUAL ENVIRONMENT?

THINK AGAIN.

Enterprises around the world are relying on virtualization to increase data center efficiency and, unknowingly, leaving themselves more vulnerable. That's because conventional security isn't able to protect virtual machines or see the traffic between them – leaving data and networks exposed. Which is why, according to Gartner Group, in 2009 sixty percent of virtual machines are less secure than their physical counterparts. But with Trend Micro™ Enterprise Security, powered by the Trend Micro™ Smart Protection Network™ infrastructure, you can mitigate the risk and maximize the benefits of virtualization. It's a different kind of security that protects your physical and virtualized environments and helps set the foundation for your company to move confidently into the cloud.

Learn how to protect your virtualized data center. Download the Trend Micro eBook at trendmicro.com/thinkagain

TREND MICRO™

Securing Your Web World

© 2009 Trend Micro Inc. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro Inc. All other company and/or product names may be trademarks or registered trademarks of their owners. *Per Gartner Group Vice President Neil MacDonald, as quoted in: McLaughlin, Laurianne, "How to Find and Fix 10 Real Security Threats on Your Virtual Servers," CIO Magazine, 14 November 2007, www.cio.com/article/print/154950 **Per Gartner Group Vice President Neil MacDonald, as quoted in: "Gartner: Rush to Virtualization Can Weaken Security," On-Demand Enterprise, 09 April 2007, http://www.on-demandenterprise.com/offthewire/gartner_rush_to_virtualization_can_weaken_security_07-29-2008_08_52_18.html

Reading Between the Lines: Progress

Call me crazy or single-minded, but this is my favorite time of year. It has nothing to do with cooling temperatures or falling leaves, but rather it's because this is when we release our annual survey, the Global State of Information Security, conducted with *CIO* magazine and PricewaterhouseCoopers.

In this month's issue, you'll find Senior Editor Bill Brenner's excellent and insightful look at this year's results. As the largest survey on information security conducted, it's a major undertaking to garner insights from the mountain of data. From where I sit, the most significant message was how far security has come over the past seven years, and how well it fared during the global economic downturn. Security teams were certainly impacted as their organizations felt the pressures of the recession, but the impact was not nearly as severe as we expected, which actually spoke to the value that businesses now place on the contributions their security teams make.

You are also getting better at understanding what's going on in your environment. We have watched a steady decrease over the past three years in the number of survey respondents who could not quantify the number of security incidents that their organization experienced, or the source of those incidents.

I was also encouraged to see the survey results from India and China. India continues to invest in top-level security technology and practices. It appears that security threats have awakened Chinese businesses as we saw a marked increase in the level of investment and best practices implementation there. It will still take time for the benefits of those actions to be recognized (nothing happens overnight), but I applaud their actions.

For the CSO profession, there was even more good news: The number of organizations with a CSO or CISO jumped significantly. Whether in response to regulatory demands, darkening threat landscapes or better support at the executive level in their role, more and more businesses decided to elevate security to a senior role and give it a seat at the table.

We've been screaming for years that businesses don't always value the role of security, but in an economic downturn where the risks are even greater and the bad guys are lining up to take advantage of unprepared businesses, we are seeing those businesses benefit from leadership, intelligence and having a security plan in place.

In the September 2008 issue of *CSO*, I challenged CSOs to "translate the value of [your] organization's investment in security into the business value that it delivers to the organization." I was either right-on or a little late, because it appears that is exactly what is happening. Increasingly, security is seen as an enabler of the business, no longer just a cost center. Congratulations. And here's to more success in the future.

Best regards,
-Bob Bragdon, bbragdon@cxo.com

Advertiser Index

3M 3
BeyondTrust 15
CA 9
CSO 17, 23, 39
DEMO C3
IBM Corp. C2
Juniper Networks, Inc. 28
Palisade Systems 12
PhoneFactor C4
Raytheon Co. 10
RSA Security 19, 21
Trend Micro Inc. 5
VeriSign 7

CSO

President and CEO
Michael Friedenberg
Group Publisher Bob Melk
Publisher Bob Bragdon
Senior National Sales Manager
Per Melker
East Coast Regional Sales Manager
Roz Burke
West Coast Regional Sales Manager
Michelle McHugh
Sales Associate
Sarah Nadeau

INTEGRATED MEDIA AND ONLINE SALES
SVP, Online Sales & Ops
Gregg Pinsky
VP, Online Sales
Brian Glynn
East Coast Online Regional Sales Manager
Richard Hartman
West Coast Online Regional Sales Manager
Erika Karr
Central Online Regional Sales Manager
Stacy Bryne
Manager, Online Account Services
Danielle Tetreault
Online Account Services Specialists
Jennifer Malkasian, Elise Ryan, Tara Shea

CUSTOM SOLUTIONS GROUP
Vice President Charles Lee
National Sales Directors
Adam Dennison, Tom Grimshaw, Karen Wilde

PRODUCTION
VP/Manufacturing Chris Cuoco
Production Manager Heidi Broadley

EXECUTIVE PROGRAMS
SVP, Executive Programs
Ellen Daly
Vice President, Event Marketing
Michael Garity
Sr. Director, Event Operations
Deb Begreen
VP, Content Development & Events
Derek Hulitzky

MARKETING
Vice President, Marketing
Sue Yanovitch
Sr. Marketing & PR Specialist
Lynn Holmlund

LIST SERVICES
Contact Steve Tozeski of IDG List Services at 508 820-8106 or *stozeski@idglist.com*

REPRINTS & PERMISSIONS
For information about reprints and copyright permissions, please contact The YGS Group, 800-290-5460 ext. 129, *cso@theygsgroup.com*

Photo by Christopher Navin

VeriSign®

FORTUNE 500 COMPANIES DON'T CHOOSE SECURITY ON A WHIM.

Over 95 percent of the Fortune 500 choose VeriSign SSL as their online security of choice. Why? Because VeriSign can enable the strongest encryption available and has the most rigorous authentication standards. Or because VeriSign® Extended Validation (EV) SSL offers the most visible site security available by displaying the green address bar in high-security browsers, which is also the most effective defense against phishing scams. Add it up, and it's easy to see why industry leaders choose VeriSign—the most trusted symbol of security on the Web.

It's powerful. It's the most visible. Learn more about protecting your site and your customers at **VeriSign.com/EVSSLPaper**.

VeriSign® Secured

TRUST THE ✓

© 2009 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle logo, the VeriSign Secured logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other trademarks are property of their respective owners.

Join the Discussion

What's on your mind? Security leaders discuss and debate at ***www.csoonline.com***

BLOG POST

Information Asset Value: Some Cold-Hearted Calculations

Many readers know this already, but about five years ago (long before I came to Forrester), Dan Geer, Kevin Soo Hoo and I founded an organization called Securitymetrics.org, devoted to the study of security metrics. I moderate a mailing list that has about 800 security researchers, CISOs, consultants and managers. Discussions are always lively!

One of the list's most active members, Meritology's Russell Cameron Thomas, just posted a thoughtful essay on how to value information assets. I liked his post very much. Russ describes an eminently sensible way to calculate business asset value. At the risk of being reductionist, it involves: 1) Figuring out the value of those assets that even the coldest-hearted business analyst would agree contribute to the top line and 2) Then figuring out the value of everything else. The sum of those two numbers is the total value.

In practice, though, the assets in the first category (the cold-hearted analyst's favorite ones) are also the scarcest. A key question would be, "did you build security into the business effort that this asset serves from the start because it was critical to customer acceptance?" I can think of exactly one example of this in my entire career where this is true. Everything else has been some flavor of a bolt-on.

Because security-as-business-enabler sightings are as rare as the abominable snowman, that means just about everything defaults into category 2. As such, to me, the easiest way to value those assets is to apply what (if I remember correctly) was Pete Lindstrom's test: The value of the asset must be worth at least what you are willing to spend to keep it secure. Lindstrom's Razor (if I can call it that) identifies a floor value of the information. It doesn't require interviews or any sort of guesswork, just a spreadsheet and a few defensible ideas about how to allocate costs that are known and can be measured.

In my book, *Security Metrics: Replacing Fear, Uncertainty and Doubt*, I recommended a similar strategy for quantifying and allocating security cost:

"Tying back security costs to business units or revenue-generating systems is more difficult. Cost allocation is, for most organizations, a black art. In fact, given the degree of political wrestling that occurs when figuring out chargeback formulas, one might more profitably call it a full-contact sport. Regardless, security organizations should try, to the best of their abilities, to associate specific expenditures with business initiative.

"Certain security costs are easy to allocate, such as outsourced security monitoring services for a demilitarized zone, single sign-on systems (SSO), application monitoring tools and external audits:

- Outsourced security monitoring services for a demilitarized zone (DMZ). (Strategy: pro rata allocation based on user sessions or bandwidth.)
- Single-sign on system. (Strategy: pro rata allocation based on deployment of SSO agents on business servers, plus labor allocation.)

MORE ON THE WEB

Making All the Right Connections?

CSO's online event board lists conferences and networking opportunities in digital and physical security, fraud prevention, business continuity and more.

See www.csoonline.com/events/index/1.

When your critical information and infrastructures are protected by Raytheon, you can be confident you have the most innovative and proven cybersecurity solutions available. No matter how complex the system or threat, Raytheon's integrated cybersecurity solutions safeguard the confidentiality, integrity and availability of critical information and infrastructures. With a track record of performance that spans decades, Raytheon is trusted by governments and Fortune 500 companies around the globe to deliver a powerful line of strategic defense – no matter the threat.

Raytheon

Customer Success Is Our Mission

EXECUTIVE VIEWPOINT

ADVERTORIAL

DLP: Keeping Intellectual Property Inside

Data loss prevention key to risk management success

Christian Renaud, CEO, PALISADE SYSTEMS

Christian Renaud is the CEO of Palisade Systems in Ames, Iowa. Palisade Systems is a leading provider of Data Loss Prevention solutions for the small and medium enterprise market.

While every organization, regardless of size, should have a risk management policy in place, knowing which components of risk management are must-haves can be challenging. One key component of risk management is data loss prevention (DLP), which, according to Christian Renaud, CEO of Palisade Systems, is all about bounding risk problems and remediating them. Read on for practical insight on how to cost-effectively prevent data loss.

> "Too many people skip into the forest and say they know what's going on when they really don't."

What are some of the most important factors to consider when implementing DLP solutions?

You need to look at the business needs and the network type, time to deployment and time to utilization. We have a comprehensive, three-tiered approach to DLP: protocol filtering, email and Web filtering, and content analysis within those protocols. DLP should be the easiest thing for IT staff to do—from initial configuration, to thorough reports, to a very seamless deployment interface. Focus on sizing the solution to fit your unique problem.

Why is data loss prevention a critical component of a risk management solution?

There's the human factor and, of course, theft. It basically comes down to visibility on your network and on your data. It's necessary to have tools that will tell you where your data is and what's going on with it so you can take informed action on it. You need to have network security and firewalls, and you need a comparable amount of focus on the data that is leaving your organization.

What kinds of costs are involved if risk is not mitigated or reduced?

The cost varies from organization to organization, based on your industry or vertical market. These range from the cost of HIPAA violations, PCI, or pure intellectual property loss like source code or trade secrets. You should apply the metrics that are relevant to your industry. A softer cost is the administrative time of this risk management solution, as your time is valuable. The bottom-line costs are often from not taking action in the first place.

What are the organizational barriers to deploying a DLP solution?

Organizational barriers are less applicable for SMBs, but the administrative domains, such as the IT domain, the implementer, the collaboration people, the application people and security people are all microboundaries in IT. Administrative staff, finance and human resources all have a liability perspective, as each discrete function has sensitive data and is a stakeholder guarding the company's assets. The difficulty in building a comprehensive risk management strategy is that the IT team deploying the solution often doesn't have perfect information to craft policies. So the IT team needs to sit down with each stakeholder to put the right policies in place.

What advice do you have for a successful DLP deployment?

Take a real sober look at where your risk is and quantify your data. What are the people, policies and systems you have in place to prevent data from getting out? It comes down to having a playbook, a process and the right people. Think through the worst-case scenario: What happens if your credit card numbers get out, even if you have a firewall? Also, take up any one vendor on their free assessment offer to get visibility into your network that you might have. The more knowledge you have about your situation, the better you can respond and structure around your risk.

Can you give an example where DLP has helped enhance existing policies and procedures?

Bank Mutual was able to see exactly what was happening in its network, and identify and prevent data loss with Palisade's tool. You can read the Bank Mutual case study at www.palisadesystems.com/common/files/BankMutual_CaseStudycso.pdf.

Palisade®
Securing your data is our business™

CSO
Custom Solutions Group

"We understand that given our wide distribution base, we're going to be a target." PAGE 20

Briefing

TRENDS, STATS AND FAST FACTS

Edited by Bill Brenner

7 Ways Security Pros DON'T Practice What They Preach

In an informal poll conducted by CSOonline, many IT security pros admitted they don't always follow their own advice

IT security pros are often driven to drink—literally—over the daily battles of their job: bosses unwilling to accept the rationale for some new security investment, employees who regularly infect their computers by doing things that have nothing to do with their jobs and vendors who don't understand the company's needs. (The latter example is examined online in "8 Dirty Secrets of the IT Security Industry": *www.csoonline.com/article/499815*.)

But in a recent, unscientific and informal poll that *CSO* conducted online over such social networks as Twitter and LinkedIn, many IT security pros admitted they've often looked the enemy in the eye only to find themselves staring back in the mirror. Or, they've seen carelessness in well-meaning professionals who should know better.

Paul de Souza, a former chief security engineer at AT&T and owner of the Cyber Warfare Forum Initiative (CWFI), has seen many examples where IT security pros fail to practice what they preach. "I have noticed that many security professionals do not encrypt their hard drive," he says. "I also see a lack of two-factor authentication deployment. Many of us security professionals rely only on passwords."

Based on the poll and a list provided by Andy Willingham, former network security engineer at EBFC, information security engineer at MARTA and founder and owner of AndyITGuy Consulting, here are seven examples of how security pros cut corners:

1. Using URL shortening services. URL shortening services have become immensely popular in recent years, especially among security pros who use such forums as Twitter to share content. The problem is that URL-shortening services are sometimes insecure and unstable. (For examples online, see "New Spam Trick: Shortened URLs and 5 More Facebook, Twitter Scams to Avoid": *www.csoonline.com/article/496920*.)

In the latter example, Graham Cluley, senior technology consultant with U.K.-based security firm Sophos, noted in a recent interview that some URL-shortening services have begun trying to filter out bad sites by checking URLs against known black lists. That issue is far from resolved, particularly because Twitter and Facebook do not have a filtering mechanism for bad shortened URLs, despite increased efforts to block malicious links.

2. Granting themselves exemptions in the firewall/Web proxy/content filter. Willingham noted that it's not uncommon for security pros to bypass the very security mechanisms they enforce on other employees, often because those mechanisms get in the way or because they are in a hurry to get a particular task done.

One senior system engineer, who isn't named due to the sensitive nature of the topic, admitted he has run several development and test systems without an active firewall or antivirus out of necessity.

3. Snooping into files/folders that they don't own. Nobody admitted outright that they have done this themselves, but Willingham and others polled said they know of cases where fellow security practitioners have gone into someone else's files. Sometimes it was because of an investigation into a security incident. Other times, it was simply a matter of having the access and being nosy.

4. Using default or easy passwords.

Threat Watch

Illustration by Joanna Szachowski

VULNERABILITY MANAGEMENT

A "Nightmare" of a Patch Tuesday

Microsoft unloads its largest security update since moving to a monthly Patch Tuesday cycle six years ago

Microsoft delivered a record 13 security updates last month that patched 34 vulnerabilities in every version of Windows, including Windows 7, as well as in Internet Explorer (IE), Office, SQL Server and other parts of its software portfolio.

The 34 flaws was also a record number for Microsoft—the most holes patched in one sitting since Microsoft switched to a regular, monthly update schedule six years ago. The closest competitor was December 2008, when the company quashed 28 bugs.

"To anyone following Apple, this isn't a big surprise," says Andrew Storms, director of security operations at nCircle Network Security, referring to Microsoft's operating system rival, which typically issues security updates that include scores of fixes. "But this is certainly an unprecedented month for Microsoft."

Microsoft ranked eight of the 13 updates and 21 of the 34 vulnerabilities as "critical"—the top rating in its four-step scoring system. The remainder of the bulletins were judged "important"—the next threat level down—while nine of the flaws were also pegged important and the final four were tagged as "moderate."

Among the October patches were several for zero-day vulnerabilities—bugs for which exploit code had already gone public.

Microsoft patched three vulnerabilities in SMB (Server Message Block) 2, a Microsoft-made network file- and print-sharing protocol that ships with Windows; two bugs in the FTP server that's included with older editions of its Internet Information Services (IIS) Web server; and two in the Windows Media Runtime. The flaws in SMB 2 and IIS had been public knowledge since early September, but the Windows Media vulnerabilities included one that Microsoft said was already in the wild, but had not leaked to the usual public sources, such as security mailing lists.

Jason Miller, the security and data team manager for patch management vendor Shavlik Technologies, describes the release as "an administrative nightmare," from the perspective of "just trying to get a good grasp of what's out there."

IT security practitioners interviewed the morning after the patch release said even though they have smoothly-working patch management programs, the October release was a bit much.

"Heavy patch months cause 'regulated' patches," says Fresno, Calif.-based network security contractor Susan Bradley. "This, in turn, causes Windows XP to not properly notify folks that use the 'notify me' function." This month, she says, more people will probably get caught with that download patch bug.

Rick Lawhorn, a Richmond, Va.-based IT security practitioner, isn't worried as much about the particular vulnerabilities patched as he is about the size of the update. "Microsoft architecture, in my opinion, does not lend itself to large updates well," he says. "Updates should be small and manageable so Microsoft can work out the dependencies first. The trade-off is a higher frequency of patches, but the reward is smaller, more controllable changes."

-Gregg Keizer and B.B.

(Continued from previous page)

Willingham noted that IT security practitioners are often guilty of giving themselves easy-to-remember passwords such as the name of their city or town, a pet's name or a favorite beverage. This, of course, flies in the face of everything we've heard about using complex passwords or nixing passwords altogether in favor of a more secure method of authentication.

5. Failure to patch. On the second Tuesday of each month, e-mail inboxes are crushed beneath the weight of advisories from vendors, analysts and others regarding the security patches Microsoft almost always releases on that day. But security practitioners say they don't always keep their systems fully patched or that they have seen others make do without some critical fixes. (See Example 5 in "7 Deadly Sins of Networking Security": *www.csoonline.com/article/470095*.) The reasons range from underdeveloped patch management systems to the simple belief that fast patching isn't the imperative some make it out to be. "I don't always keep my own systems patched/updated," said the anonymous security practitioner first mentioned in example two.

6. Using open wireless access points. IT security practitioners know it's not always safe to latch on to the wireless network at an airport, coffee shop or conference (including Black Hat and Defcon, where Wi-Fi hacks have become legendary), but when one needs to read some crucial e-mail, check on problems with a webpage or simply stave off boredom, the nearest Wi-Fi is often good enough.

7. Misuse of removable storage devices. Security practitioners often complain that employees lose removable storage devices containing sensitive data on airplanes, buses and curbsides. But Willingham says security pros are often just as guilty. *-Bill Brenner*

Photo by Veer

Three Platforms.
One Provider.
Complete Privileged Access Control.

Introducing the new BeyondTrust.

A security strategy is only effective if it grows with your company. As enterprises deploy more Linux®, UNIX®, and Windows® in heterogeneous IT environments, managing sensitive data in these multi-platform infrastructures can be difficult, complex, and costly.

Meet the new BeyondTrust, a leading provider of Privileged Access Lifecycle Management solutions for heterogeneous environments. Our leading products protect sensitive and confidential data through an effective combination of privilege delegation, strict user access control, privileged password management, and secure audit trails. With solutions that prevent data breaches and achieve regulatory compliance, hundreds of Forbes 2000 companies rely on us to maximize their security while reducing complexity and administrative costs.

Try it free for 30 days at www.beyondtrust.com/cso

When it comes to managing risk, we have the key.

beyondtrust®
Control Access. Control Risk.

Copyright© 2009 BeyondTrust Software International, Inc. All rights reserved. BeyondTrust is a trademark of BeyondTrust Software International, Inc. UNIX is a registered trademark of The Open Group. Linux is a registered trademark of Linus Torvalds. Windows is a registered trademark of Microsoft Corporation. All trademarks are registered in the United States and/or other countries.

1-800-234-9072

Q&A

Why Pen Testing Is Central to Pennsylvania

Commonwealth of Pennsylvania CISO **Robert Maley** explains why penetration testing has become an essential tool in his security arsenal

Fortify Cofounder and Chief Scientist Brian Chess created a stir last year when he predicted—incorrectly, so far—that penetration testing would be a dead art in 2009. Among those who shrugged off the suggestion was Robert Maley, CISO for the Commonwealth of Pennsylvania.

Maley—a customer of Core Security Technologies—explains how pen testing became an essential piece of his strategy to keep citizens' personal data out of enemy hands.

Given that you're processing cardholder data online, what have you had to do to meet the demands of PCI security compliance?

Maley: We don't store cardholder data here, but we do handle the transactions that are then passed onto the bank. This is where penetration testing is important. We use internal vulnerability scanning to find and mitigate vulnerabilities before bringing in an outside vendor for additional scanning. We've had a lot of success with this approach so far.

Describe how pen testing has been woven into your core security procedures.

We have what's called CA2—Commonwealth Application Certification and Accreditation—patterned after the Department of Defense's accreditation process for systems. We focus ours on Web-based applications. One of our challenges is that, like a lot of organizations, we have to be mindful that a lot of Web-based apps are the target of cross-site scripting and SQL injection attacks.

Here in the Commonwealth, we've had applications developed for years and years with no real underlying security process. So we have to constantly search for things that can be exploited and mitigate the problems before something happens. The bad guys are escalating their SQL injection attacks. We see these attacks constantly, in the thousands. Why are they doing that? Because there are so many vulnerabilities out there and they know they can eventually hit something.

Was CA2 designed to find the flaws left over time or to catch flaws during the development of newer apps?

It injects security in at the very beginning of a project now. Whether a Web application is developed in-house or outsourced, it now has to go through the CA2 process before going live. Part of that process is that the programs have to be pen tested.

Describe what your pen testing schedule typically looks like.

We don't randomly go out and pen test things. We don't have that kind of time. We use it at a specific point in the CA2 process. We also use it as a specific piece of the compliance process. In the meantime, if we suspect something like an SQL injection attack against a certain app, we go back and do pen testing.

One innocuous webpage with job descriptions was subject to such attacks. Through pen testing we were able to extract info about every state employee and their dependents through that page. So we shut it down and did a thorough investigation. We keep all our log files and were able to pinpoint the point in time where attackers started trying to target the data. That's the kind of success we have had.

–B.B.

CCTV

Taking the "Closed" Out of Closed Circuit

CCTV SURVEILLANCE systems are notoriously proprietary. (The circuits are "closed," after all.) The IP networking protocol is generally thought of as an "open" system—but that doesn't mean all IP-based surveillance devices work together. Members of the Physical Security Interoperability Alliance (PSIA)—a consortium of approximately 50 physical security product providers—continue to tackle the issue of interoperability between IP-enabled security technologies. The group recently released a draft of what it hopes will become the second specification to standardize IP-enabled video platforms.

The Recording and Content Management (RaCM) draft specification builds on a specification released earlier this year that created standards for how a video stream goes from a camera to viewers or recording devices. This latest RaCM specification would standardize the way recording and content management products communicate with other devices in the security ecosystem, according to Dave Fowler, PSIA member and senior vice president of marketing and product development with VidSys, who cochairs the RaCM working group.

"This second area is: If you send video to a recording device, how does the device handle storing it, playing it back and being able to create metadata so you can find it again?" says Fowler.

Fowler says the goal is for recording devices and video management systems to enable users to have a single video management system to view recorded video. The end result, he says, would reduce significant headaches and expensive changes that are necessary now because there is currently no interoperability protocol for existing DVR and NVR solutions.

–Joan Goodchild

CSO Perspectives

SAVE THE DATE

April 5-7, 2010
Hyatt Regency Santa Clara
Santa Clara, California

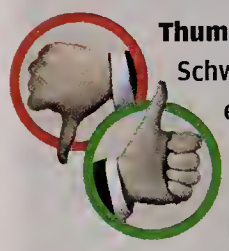
The 2010 CSO Perspectives™ conference is the landmark peer-to-peer event for senior security executives.

www.csoonline.com/events
800-366-0246

Produced by:

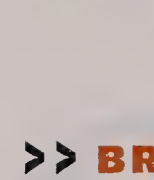
CSO
BUSINESS RISK LEADERSHIP

Security Wisdom Watch

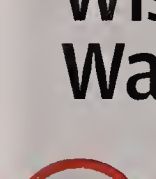


Thumbs both ways: Arnold Schwarzenegger. The Governator was criticized after he vetoed an update to California's landmark data-breach notification law, saying the new bill would be too hard on businesses without adequately benefiting consumers. Some businesses would argue he's right.

Thumbs down: Jason Miller, security and data team manager for patch management vendor Shavlik Technologies. Sure, Microsoft's October Patch Tuesday update was the largest ever. But Miller helped nobody by throwing around such FUD-laced descriptions as "administrative nightmare."



Thumbs up: Dow Chemical Company. The company deserves credit for its Transportation Community Awareness and Emergency Response leadership. The national outreach effort brings chemical and transportation industry experts into local communities to provide free transportation and chemical safety training to emergency personnel.



Thumbs down: We the People. Our addiction to social networking sites like Facebook and Twitter is causing us to willingly abdicate our privacy rights. We have met the enemy, and it is us.

Thumbs up: Adobe. Because the company blatantly copied Microsoft's patch release process, users may actually have an easier time improving their app security from now on.

-B.B.

LEADERSHIP

2009 WOMEN OF INFLUENCE AWARD WINNERS NAMED

These awards honor accomplished, inspirational women in information security, risk management and privacy

The 2009 Executive Women's Forum "Women of Influence" (WOI) awards were awarded recently at the event in Scottsdale, Ariz.

The awards were copresented by Alta Associates and *CSO* magazine, recognizing women in four categories: the public sector or academia, a private solutions provider from the security industry, a corporate practitioner from the private sector and a "One to Watch"—a future leader in the security field. The winners were nominated by peers in the security community.

Mischel Kwon

This year, the public sector winner is **Mischel Kwon**, outgoing director of the U.S. Department of Homeland Security's Computer Emergency Readiness Team (US-CERT).

Kwon, an IT professional with more than 26 years of experience, recently joined RSA's Worldwide Professional Services unit as vice president of public sector security solutions.

She previously served with the United States Department of Justice, where she was deputy director for IT security staff.

Patricia Titus

The 2009 private solutions provider winner is **Patricia Titus**, chief information security officer with Unisys.

Prior to her position with Unisys, Titus served for six years with the Transportation Security Administration where she created, implemented and maintained a robust IT security program and led her team to have an IT security program rated with a Federal Information Security Management Act compliance score of "A" for 18 months.

When she joined Unisys Federal Systems as the chief information security officer, she brought much of that rigor to its security program, according to her nomination.

This year, the winner in the WOI corporate category is **Michelle Dennedy**, chief governance officer for Sun Microsystems.

Dennedy is seen as a creative leader in changing the view of privacy from that of strict regulation to one of social responsibility, according to her nomination. In addition to raising the visibility of data privacy and data integrity issues to all of Sun's engineering and field employees, Dennedy has been a staunch advocate of processes to incorporate that awareness into best practices, ranging from laptop encryption to evaluation of privacy standards in acquired companies.

The 2009 "One to Watch" winner is **Char Suter**, SVP of information security with HSBC North America. According to Suter's nomination, while she is a relative newcomer to the information security field, she has embraced it with a passion and made a tremendous difference at HSBC.

Suter has made significant contributions to an HSBC Identity and Access Management program that was launched two years ago.

-J.G.

Verbatim...

Shots heard 'round the security world

"This is an administrative nightmare, just trying to get a good grasp of what's out there."

-Jason Miller, security and data team manager for patch management vendor Shavlik Technologies, on the massive number of security updates Microsoft released in October. Thirteen separate bulletins addressed 34 vulnerabilities.

"Your credit card company and your loyalty card program memberships track your purchases, travels, expenditure levels, and blend that into offers that meet your lifestyle profile. Firms sell GPS devices specifically to be hidden in vehicles, permitting anyone to track your movements. The RFID Tollway passes [that] states offer [can] speed you through their toll roads, know where you've been and how fast you drove."

-John Zurawski, vice president of Authentify, on why the privacy of individuals is quickly evaporating

"Google says one thing when trying to sell its products, but something else in federally required filings aimed at shareholders."

-Consumer Watchdog advocate John Simpson, faulting Google for "blandly assuring" customers about the security of its cloud-based services while at the same time warning of multiple security risks in federally required 10-Q financial statements

You want an authentication solution that's rock-solid.
Shouldn't you expect the same of the company behind it?

www.rsa.com

RSA
The Security Division of EMC

©2009 RSA Security Inc.

BY THE NUMBERS

6

Years since Microsoft started the monthly security update schedule known as Patch Tuesday

400

Patch Tuesday security bulletins in that period

745

Vulnerabilities fixed in that period

13

Security bulletins that Microsoft released for October

34

Vulnerabilities that the 13 updates are meant to fix

29

Flaws addressed in the October mega-patch that Adobe released on the same day as Patch Tuesday

PATCH MANAGEMENT

After Attacks, Adobe Patches Now Come Faster

Hackers like Adobe Systems, and now the company knows it all too well.

Adobe's software has increasingly come under attack in recent years as hackers have come to realize that it can be easier to find flaws in popular software that runs on top of Windows than it is to dig up new vulnerabilities in the operating system itself.

That's led to a round of new attacks that exploit bugs in products such as Adobe's Reader, Apple's QuickTime and the Mozilla Firefox browser, for example.

It's a reality that Adobe Chief Technology Officer Kevin Lynch freely acknowledged during the company's annual Adobe MAX developer conference in Los Angeles last month.

"We have absolutely seen an increase in the number of attacks around Reader in particular, and also Flash Player to some extent," he said. "We're working to decrease the amount of time between when we know about a problem and when we release a fix. That used to be a couple of months; now it's within two weeks for critical issues."

For Adobe, this new reality became clear in February, when the company's Reader and Acrobat software were the targets of a widespread attack. The volunteer watchdog group Shadowserver Foundation started sounding the alarm about the problem Feb. 19. And though security experts later determined that it had been exploited by attackers since early January, Adobe didn't end up patching its bug until March 10. It took two more weeks for the company to patch all of its supported platforms.

It was a public relations disaster for the company, whose sluggish response was pilloried by security experts.

Adobe Director for Product Security and Privacy Brad Arkin says the problems spurred good things, though. "We used that experience to help understand where the bottlenecks were and what process changes we could implement to improve our response time," he says.

In May, Arkin announced that the company would take new steps to stress-test its software and improve its response-time to security incidents.

Now Adobe releases regularly scheduled security software updates like Microsoft and Oracle, but if it needs to rush out a patch, it can do this much more quickly than before.

Adobe posted emergency patches in May and again at the end of July, both of which took about two weeks to turn around, Arkin says. "The turnaround for these things is something that has been a real focus," he says.

"We understand that given our wide distribution base, we're going to be a target," according to Arkin. "These types of software patches are going to be a fact of life for us."

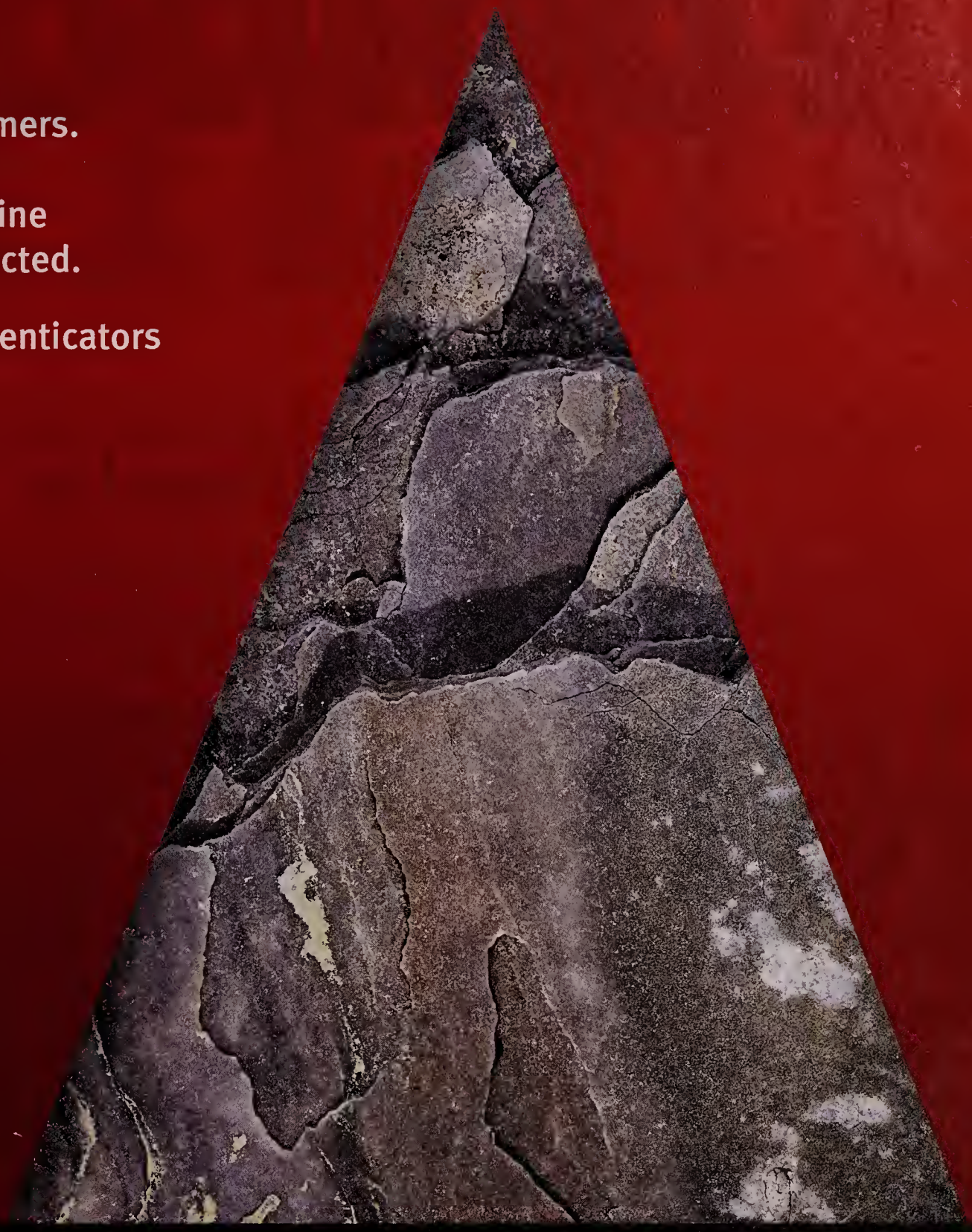
-Robert McMillan

Illustration by Joanna Szachowski

34,000+ customers.

200 million online identities protected.

40 million authenticators deployed.



For an authentication solution that is truly strong,

Find security in RSA.

RSA®

The Security Division of EMC

www.rsa.com

Security Information and Event Management | Data Loss Prevention | Identity & Access Management

©2009 RSA Security Inc. All rights reserved. RSA and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and other countries.
EMC is a registered trademark of EMC Corporation.

Toolbox

TOOLS, TECHNOLOGIES AND TACTICS

By Mary Brandel

Patching Things Up

Software can automate parts of the patch management process—but not all of it. Here's how to choose the right system and get the most from it.

Patch management software helps organizations acquire, test and install code to fix known vulnerabilities in operating systems and applications. It also helps them assess exposure and prioritize patches (given your specific environment), identify missing patches that need to be remediated and produce real-time reports for compliance and other auditing needs.

Since its emergence early this decade, patch management has become "operationalized," says Ronni Colville, an analyst at Gartner. For instance, the function is being subsumed into PC configuration management vendors' suites, such as Symantec (Alterus) and Avocent (LanDesk). However, she says, in most cases, these systems don't offer the richness of capability provided by point solutions.

Three main players remain in the point solution market: BigFix, Lumension and Shavlik. Still, Colville says, "no vendor can make a full business on just patch management, so they've brought in other functions." For instance, BigFix has broadened its security focus to include more configuration functions (such as inventory and software distribution), she says, while Lumension and Shavlik have begun to include functions such as security configuration, endpoint vulnerability assessment, and data leakage prevention.

Meanwhile, some companies continue to use Microsoft Windows Server Update Services (WSUS) to patch Windows operating systems and applications because it's free, but it's also more manually intensive.

Range of Capabilities

A full-featured patch management system should do the following:

Research: Receive information about new patches from vendors and push this information to the patch server.

Asset discovery: Scan the network to produce a full inventory of IT assets, and provide flexible ways to group and classify these assets.

Vulnerability assessment and prioritization: Identify vulnerabilities based on the specific endpoints in the environment and rank them in terms of which will have the most impact and which are most important to address.

Remediation: Continuously deploy,

Illustration by Steve Munday

SECURITY Smart™ NEWSLETTER

THE EMPLOYEE SECURITY AWARENESS NEWSLETTER FROM THE EDITORS AT *CSO*

Security Smart is a quarterly security awareness newsletter ready for distribution to your employees—saving you precious time on employee education! The compelling content combines personal and organization safety tips so is applicable to many facets of employees' lives. And the easy to read design has multiple entry points so you are assured that your intended audience of employees—your organization's most valuable assets—will read and retain the information.

SECURITY Smart™ NEWSLETTER

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

Have a Safe Trip!

Experts say when you travel, staying "relaxed but alert" can help you anticipate and avoid trouble.

DAVID KATZ, CEO OF THE GLOBAL Security Group, leads classes on travel security and suggests that employees should maintain a state of "relaxed alertness" when traveling. He defines that as being aware of your surroundings and taking note of what is out of place. Katz also suggests a few small habits to keep your trip safe.

For example, if you go the same location repeatedly, vary your route. Leave each day at a different time. If you wouldn't wear your Cartier watch in the lower west side of Manhattan, don't flash it around a village in Bangladesh.

When booking a hotel room, request a room on the third floor or below. Fire ladders don't go above the seventh floor, and if you have to jump, any jump that's more than three times your height can result in serious injury. Take a minute to find the emergency exits and the stairwells. Start at your door and count the doors to the exit, in case of a fire, you'll want to be able to get to that stairwell even if the smoke prevents you from seeing it. The hotel should have a secure well-lit parking lot that you can leave your vehicle in, and you should feel safe walking to that lot at night.

Katz suggests choosing a rental car with low mileage over a high-mileage vehicle-even if it isn't the type you prefer. You should also remove, or ask the rental company to remove, any stickers or other markings on the car that signal it's a rental. There's no need to identify yourself as a visitor who may be unfamiliar with his surroundings (and an easy target for a thief).

Finally, employees should always leave a copy of their travel itinerary both at home and in the office. Make arrangements for regular check-in calls at home and work. If you fail to call, your co-workers and family will know to follow up.

DID YOU KNOW?

The 10 Most Dangerous Cities in the U.S.

International travel is not the only time that business travelers need to be aware of safety issues. Based on murder, rape, robbery, aggravated assault, burglary and motor vehicle theft rates the following U.S. cities were ranked as the most dangerous in 2006

1. St. Louis, MO
2. Detroit, MI
3. Flint, MI
4. Compton, CA
5. Camden, NJ
6. Birmingham, AL
7. Cleveland, OH
8. Oakland, CA
9. Youngstown, OH
10. Gary, IN

FALL 2007 Security Smart 1

Subscribe today!

To view a sample issue of the newsletter, learn about the delivery options and to subscribe visit:
www.SecuritySmartNewsletter.com

For more information please visit
www.SecuritySmartNewsletter.com

Security Smart is published by CSO, a business unit of CXO Media. © 2007 CXO Media Inc.

CSO
BUSINESS RISK LEADERSHIP

monitor, detect and enforce patch management policies.

Reporting: Provide real-time reports that satisfy the needs for auditing, compliance and management oversight.

Evaluation Criteria

The following are criteria to consider when choosing a patch management system:

- Range of operating systems supported (Microsoft, Unix, Linux, Mac OS, etc.)
- Range of applications supported (Adobe, Mozilla, RealNetworks, Apple, Java)
- Agent-based or agentless
- Types of real-time reporting available (patches deployed, when, by whom, to which endpoints, etc.)
- Scalability
- Ability to operate on low-bandwidth or globally distributed networks
- Ability to manage computers on or off the network
- Change control (ability to change settings back, pause deployments, etc.)
- Licensing options (subscription-based, perpetual or both)
- Ease of use
- Integration with other security and configuration management systems and capabilities

Prime Considerations

Configuration management versus patch management. A primary decision is whether to turn to a configuration management system for its patch capabilities or to a point product that may or may not also offer configuration capabilities. According to Colville, the reasons organizations choose the latter is they're not ready to commit to a full lifecycle configuration suite, or their current configuration management tools don't provide a best-of-breed patch management capability. The trade-off of having both in your environment, of course, is the need to deal with multiple agents and consoles.

Eric Maiwald, an analyst at Burton Group, suggests first evaluating your configuration management system for its patch management capabilities, since it might be advantageous and less expensive to maintain the same architecture for both functions, especially if it already works well in your environment. However, if you change your mind, the functionality will be more difficult to remove because the single-vendor approach means the software is embedded more deeply into your architecture.

Agent versus agentless. As Shavlik explains, agentless systems are based on push technology and on a centralized design. Server-based software scans the machines in the enterprise and initiates all actions on those machines. With agent-based solutions, client-based software scans the machine and communicates its findings back to the central console.

Agentless systems are best for networks with large amounts of bandwidth and connected machines. Agent-based systems are best for environments with frequently disconnected machines, such as mobile PCs, and distributed networks with remote locations that have limited bandwidth.

"With an agent-based system, you get more operational control and better ability to do inventory scanning and monitoring," Colville says. "What you give up is ease of deployment and more management effort, and you'll pay a higher price."

DOs and DON'Ts

DO decide between agent-based or agentless. Mark Starry, director of enterprise architecture at Concord Hospital in Concord, N.H., decided on an agent-based system from BigFix in 2004 because he thought it would better fulfill his compliance needs. The system enables him to report in real time on which patches were actually installed, not just which patches were deployed. Although it's unlikely, he would also be able to detect whether a user uninstalled a patch. He also found the BigFix agent to have a smaller footprint than other options at the time.

Starry also finds it useful that the agent can report on what software is installed on which PC, not just what is listed in the registry. "We know in a second which of our 5,000 machines are vulnerable, so we're able to react that much more quickly," he says. He can also scan the network and subnets to discover any rogue machines, since it's the corporate standard for all PCs to have BigFix on them.

Meanwhile, at Tamiyasu, Smith, Horn and Braun Accountancy, Susan Bradley, a CPA who also oversees the firm's computer systems, runs a small business server network with fewer than 50 desktops attached. She chose Shavlik's agentless system because most people are attached to the network, and even people who access the network from home are not making a full VPN connection. "I don't have to worry about laptops because they don't have that much connectivity into the network to be a risk, and their patch status is irrelevant," she says.

DO evaluate the vendor's nonpatch capabilities. Patch management is only 40 percent of what BigFix does, Starry says. He also uses the BigFix system for endpoint protection, Windows firewalls, software asset management and power management.

But not everyone wants all those capabilities through a single system. Ray Jacob, director for network and systems management for the New York City Department of Housing Preservation and Development (HPD), likes that he has multiple engineers with different network skill sets. "The people I have running Cisco security are different from the people running McAfee, which is different from Lumension," he says. "I like the fact that we have a mix of people who are all contributing here."

DO consider your architectural requirements. Some systems operate better in highly distributed environments, on large networks or in small environments. At Concord Hospital, one BigFix server manages 4,700 PCs and 400 servers, Starry says, although the system can scale to 250,000 endpoints. Colville agrees that a strength of BigFix is its scalability. "It can play in very

Agentless systems are best for networks with large amounts of bandwidth and connected machines. **Agent-based** systems are best for environments with frequently disconnected machines, such as mobile PCs, and distributed networks with remote locations that have limited bandwidth.

Sample Patch Management Systems

VENDOR	OS SUPPORTED	AGENT LESS OR AGENT-BASED	RANGE OF CAPABILITIES
Lumension *www.lumension.com*	Windows platforms (including 98, NT, 2000, 2003, XP, Vista, Server 2008), Mac OS X, CentOS, HP-UX, IBM AIX, Novell SUSE Linux, Oracle Enterprise Linux and Sun Solaris	Agent-based	Vulnerability assessment/patch management; endpoint protection (application control); data protection (device control, encryption); asset discovery; risk/compliance management
Shavlik *www.shavlik.com*	Windows platforms, including NT 4.0, 2000, XP, Vista and Server 2003	Both	Risk/compliance management; configuration management; patch and spyware/malware assessment, remediation and management
BigFix *www.bigfix.com*	Windows, Mac OS X, Solaris, IBM AIX, IBM zLinux, HP-UX, VMware ESX Server, Red Hat Enterprise Linux, Novell SUSE Linux Enterprise, Red Hat Linux and Fedora Linux	Agent-based	Systems lifecycle management (asset discovery, OS deployment, patch management, power management, software distribution); security configuration/vulnerability management; endpoint protection (antivirus, antimalware, firewall, device control, Web protection); software asset management

large or very small organizations."

Meanwhile, at HPD, Jacob needed a system that could stretch across multiple distributed points. HPD was able to distribute Lumension servers in five boroughs in New York City, with the main server at the primary data center in downtown Manhattan. "Endpoints are able to pull from a distributed point that's the shortest hop away and sometimes even in the same building as the PCs are located," he says.

At Tamiyasu, Bradley liked the fact that Shavlik was "nimble and lightweight. Others are very enterprise-tailored," she says. "I couldn't dedicate the database and hardware resources required."

DON'T expect to "set it and forget it." According to Jacob, just because you hear the word "automation" doesn't mean you can click "enable" and let the system do the rest. In addition to creating a careful and thorough test methodology, "you have to tweak, control and plan deployments and do compatibility testing," he says. For instance, when you look at a report that shows a certain number of patches didn't get applied, you need to see why that happened and then redeploy them. At HDS, one engineer is a dedicated Lumension administrator, managing the deployments, tests, feedback and remediation actions, Jacob says. "I would say 30 percent to 40 percent of his time is devoted to the patch management process," he says. "It does require man-hours, as well as always keeping risk in perspective."

DON'T overlook testing. The vendors perform some internal testing before bundling up and distributing patches. However, this is mainly focused on determining whether the patch breaks standard software and verifying that it does what it claims to do, Maiwald says. For example, Starry says, BigFix provides quality assurance on the patches before releasing them. "If a patch is issued on Patch Tuesday, it's in our hands by midnight or 1:00 a.m. or 2:00 a.m.," he says. Patch Tuesday is the second Tuesday of each month when Microsoft releases its patches.

This does not, however, take the place of regression testing you'll need to do on-site, Maiwald says. "The vendor doesn't test all the possible permutations of what is going to happen when it's applied." The stakes get higher as the environment grows. "It's one thing to push a patch out to 10 clients, but it's a bigger deal with 1,000 or 10,000," he says. Each enterprise needs to determine the level of testing required for different situations, Maiwald says, as well as the level of change management needed.

After Jacob receives the monthly patch bundle from Microsoft via Lumension, there's a 10-day compatibility testing process. During that time, the operating system engineer attends a Microsoft webinar and uses Lumension to evaluate the security bulletins that Microsoft releases against HDS's environment. The engineer then determines which patches are most relevant to deploy and distributes those to engineers in several test environments. The test environments are given five days to respond with the risk the patch imposes. A red signal means the patch broke something in the environment, yellow means there are warning signs and some support is needed, and green means the patch can be sent out in a general deployment.

Even then, Jacob says, they don't deploy to all 2,600 PCs at once. "For the first week, we might do 200 a night," he says. "We're still hedging because the testing might have missed something." It's important, he says, to minimize and control the impact so you can remediate quickly and continue your security operations without being too disruptive to the business. "It's amazing how easily things can break," he says.

Once all this is finished, Jacob says, it's almost time for Microsoft's next Patch Tuesday.

DO look beyond Windows applications. According to the SANS Institute, unpatched desktop applications such as Adobe Acrobat Reader, Microsoft Office and Apple QuickTime pose a bigger threat to organizations than unpatched Windows operating systems. On average, major organizations take at least twice as long to patch client-side vulnerabilities as they take to patch operating system vulnerabilities, SANS says.

"Just about every software application may require patching, either for security or a functionality update," Maiwald says. The question is whether it's sufficient to rely on users to do that individually or if you want something more centralized or controlled.

When Starry first implemented BigFix, it was primarily for Windows; however, "since then, my criteria have changed—I want to patch everything," he says. Using BigFix, he can integrate Java, Acrobat, Flash and custom patches into his patch management process. Similarly, Bradley patches not just Windows but also Exchange and SQL Server. ■

Mary Brandel is a frequent contributor to CSO. *Send feedback to Editor Derek Slater at* dslater@cxo.com.

The Global State of Information Security

Our **seventh-annual survey** with PricewaterhouseCoopers finds security leaders struggling to defend new platforms, from **social networking** to **cloud computing**

By Bill Brenner

TODAY'S MOST COMPELLING technologies are giving you the biggest security headaches. Social networking sites such as Twitter, Facebook and LinkedIn enhance collaboration and help your company connect with customers, but they also make it easier than ever for your employees to share customer data and company secrets with outsiders.

Virtualization and cloud computing let you simplify your physical IT infrastructure and cut overhead costs, but you've only just begun to see the security risks involved. Putting more of your infrastructure in the cloud has left you vulnerable to hackers who have redoubled efforts to launch denial-of-service attacks against the likes of Google, Yahoo and other Internet-based service providers. A massive Google outage earlier this year illustrates the kind of disruptions that cloud-dependent businesses can suffer.

But there's also good news. Even though the worst economic recession in decades has compelled you to spend less on outsourced security services and do more in-house, your security budget is holding steady. And more of you are employing a chief security officer.

Such are the big takeaways from the seventh-annual Global Information Security survey, which *CSO* and *CIO* magazines

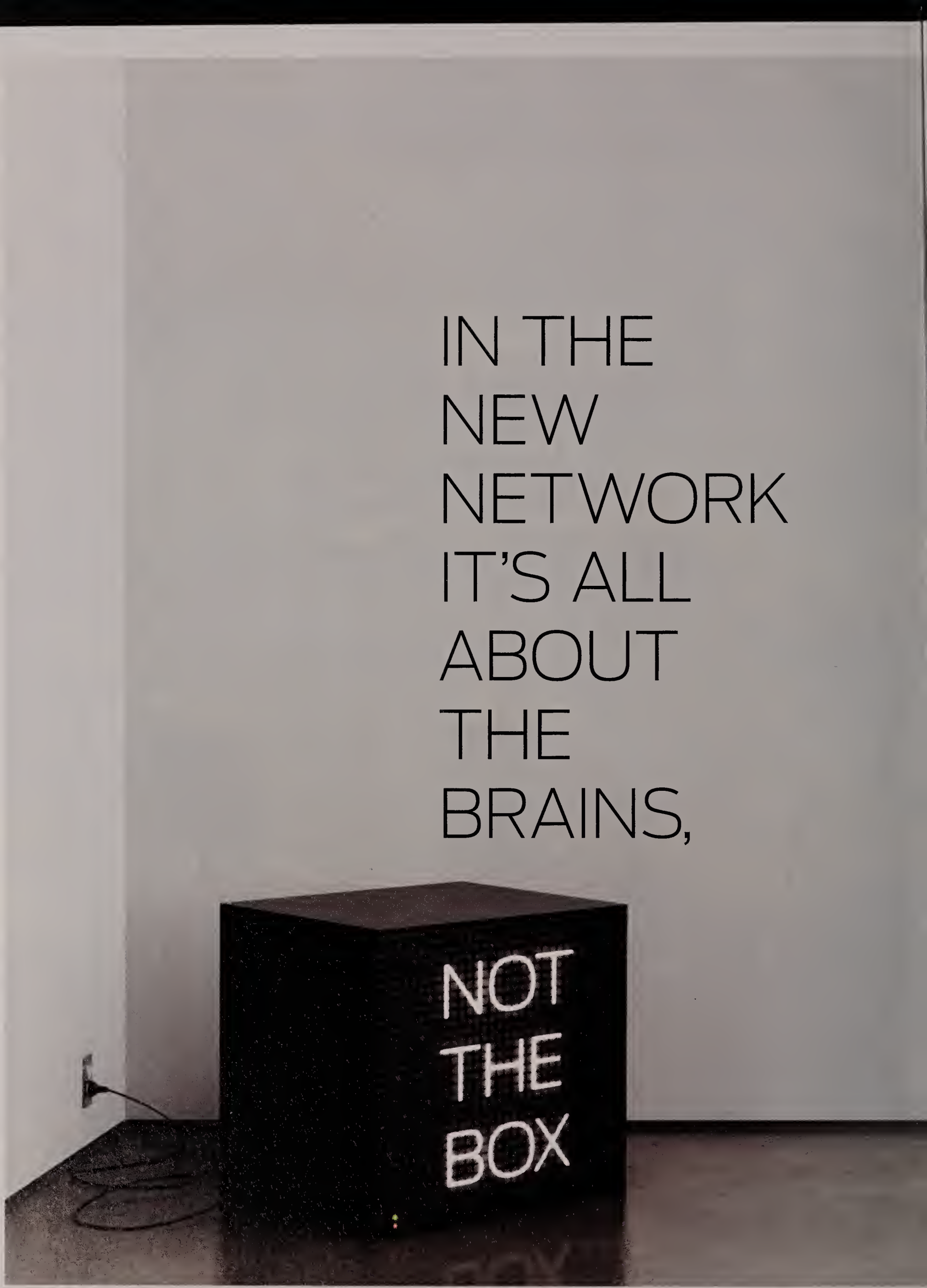
Top IT Security Priorities

New investments are focused on protecting data, authenticating users

1. Biometrics
2. Web content filters
3. Data leakage prevention
4. Disposable passwords/smart cards/tokens
5. Reduced or single-sign-on software
6. Voice-over-IP security
7. Web 2.0 security
8. Identity management
9. Encryption of removable media

Photo by Veer

IN THE
NEW
NETWORK
IT'S ALL
ABOUT
THE
BRAINS,



The challenges raised by the massive increase in networked devices and their escalating bandwidth demands will not be solved by more hardware, but by a radical rethink in the way networks work.

It calls for a whole new philosophy and that's where Junos® comes in.

THE SOLUTION

A revolutionary combination of software, silicon and systems architecture. It's how to make the box smarter. And it's only from Juniper Networks.

Junos is more than an operating system. It's the open-standards, integrated and familial approach to network design at the heart of Juniper routers, switches and security devices. It's a game changer because it brings stability to an environment that has been rife with interoperability issues. Because it creates a platform for third-party innovation and development, and because, in concert with the Junos One family of processors, it enables a new network architecture that is simpler and more powerful than anything before it.

The result is open, interoperable software-powered networking that is scalable, secure and automated.

The new network is here.
And it's running Junos.

Juniper® NETWORKS

TheNewNetworkIsHere.com

conducted with PricewaterhouseCoopers earlier this year. Some 7,200 business and technology executives worldwide responded from a variety of industries, including government, health care, financial services and retail.

These trends are shaping your information security agenda.

"I have seen examples where companies are making bigger investments in training over time to make internal staff more security savvy," says Miguel Lopez, a Los Angelas-based IT security practitioner who has worked for such companies as MSC Software and Stamps.com. Part of the reason is that regulatory compliance pressures have jolted open the eyes of top brass who may have been blind to their internal security needs previously. Lopez points to one of his friends in the industry for an example of how things have changed. "My friend, an information security manager, sits on an executive security committee with doctors and other non-IT personnel," he says. "Security is being heard from and listened to more now than ever before."

Read on to learn what we found.

TREND #1

The Promise and Peril of Social Networking

IN LESS THAN two years, social networking has gone from an abstract curiosity to a way of life for many people. When someone updates their status on Twitter, Facebook or LinkedIn, they might do it at work by day or on company-owned laptops from home at night.

What gives IT executives heartburn is the ease with which users could share customer data or sensitive company activities while they're telling you what they're having for lunch. Cyberoutlaws know this and use social networks to launch phishing scams. In one popular attack, they send their victims messages that appear to be coming from a Facebook friend. The "friend" may send along a URL they insist you check out. It may be pitched as a news story about Michael Jackson's death or a list of stock tips. In reality, the link takes the victim to a shady website that automatically drops malware onto the computer. The malware goes off in search of any valuable data stored on the computer or wider company network, be it customer credit card numbers or the secret recipe for a new cancer-fighting drug.

23%

Companies that have policies for using Web 2.0 technologies and social networking sites

It's no surprise, then, that every IT leader surveyed admitted they fear social-engineering-based attacks. Forty-five percent specifically fear the phishing schemes against Web 2.0 applications.

Nevertheless, for many company executives, blocking social networking is out of the question because of its potential business benefits. Companies now clamor to get their messages out through these sites, so the challenge for CSOs is to find the right balance between security and usability.

"People are still incredibly naïve about how much they should share with others, and we have to do a better job educating them about what is and isn't appropriate to share," says H. Frank Cervone, vice chancellor of information services with Purdue University Calumet. "We have to do a better job of enhancing our understanding of what internal organization information should not be shared."

But in a university setting, it's critical to engage people through social media, Cervone adds. Even in the commercial sector, he doesn't see how organizations can avoid it.

And yet this year—the first in which we asked respondents about social media, only 23 percent said their security efforts now include provisions to defend Web 2.0 technologies and control what can be posted on social networking sites.

One positive sign: Every year, more companies dedicate staff to monitoring how employees use online assets—57 percent this year compared to 50 percent last year and 40 percent in 2006. Thirty-six percent of respondents monitor what employees are posting to external blogs and social networking sites.

To prevent sensitive information from escaping, 65 percent of companies use Web content filters to keep data behind the firewall, and 62 percent make sure they are using the most secure version of whichever browser they choose. Forty percent said that when they evaluate security products, support and compatibility for Web 2.0 is essential.

Unfortunately, social networking insecurity isn't something one can fix with just technology, says Mark Lobel, a partner in the security practice at PricewaterhouseCoopers.

"The problems are cultural, not technological. How do you educate people to use these sites intelligently?" he asks. "Historically, security people have come up from the tech path, not the sociologist path. So we have a long way to go in finding the right security balance."

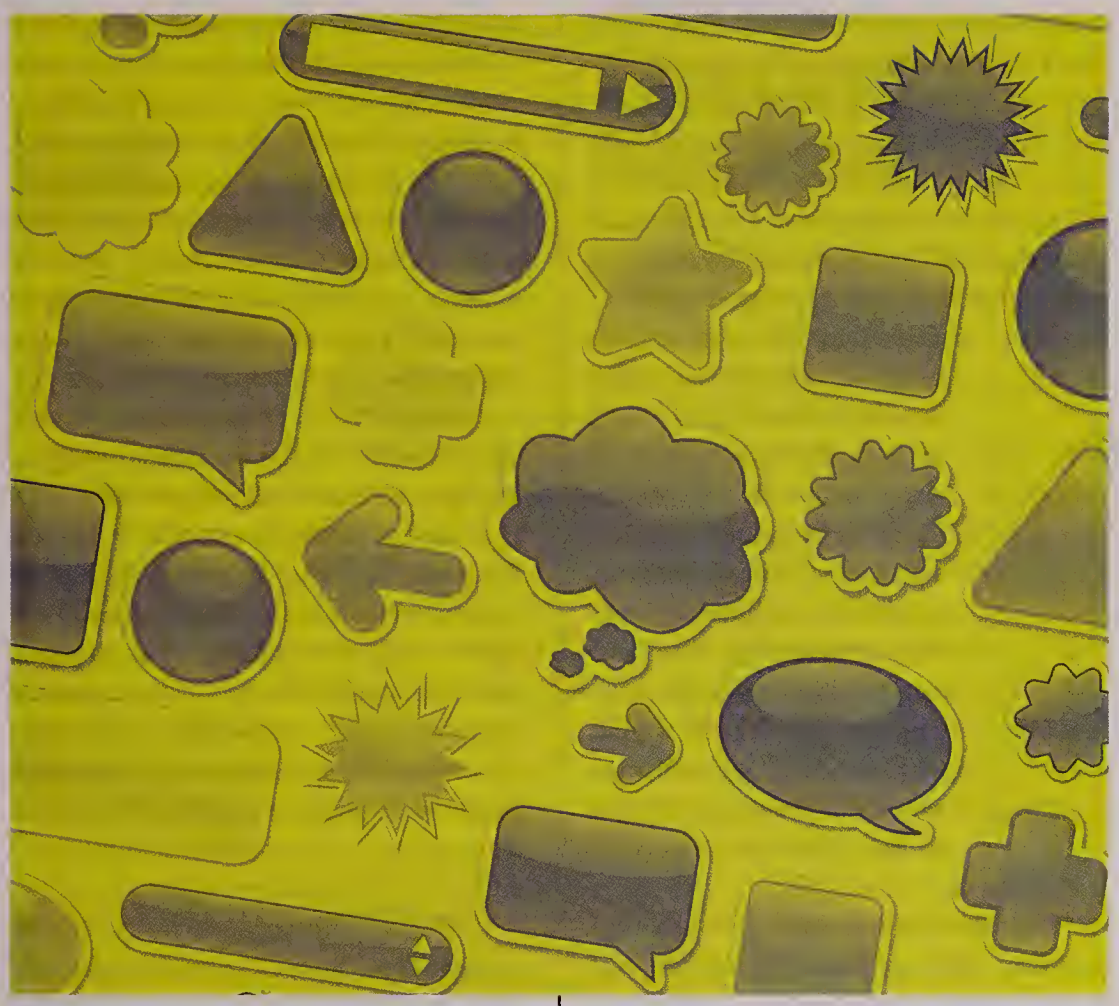
Guy Pace, security administrator with the Washington State Board for Community and Technical Colleges, says his organization takes many of the precautions described above. But he agrees with Lobel that the true battleground is one of

Dark Cloud

Fears about vendors dominate cloud security risks

WHAT IS THE GREATEST SECURITY RISK TO YOUR CLOUD COMPUTING STRATEGY?

23%	Ability to enforce provider security policies
22%	Inadequate training and IT auditing
14%	Access control at provider site
12%	Ability to recover data
11%	Ability to audit provider
10%	Proximity of company data to someone else's
4%	Continued existence of provider
4%	Provider regulatory compliance



office culture, not technology. "The most effective mitigation here is user education and creative, effective security awareness programs," he says.

TREND #2

Jumping into the Cloud, Sans Parachute

GIVEN THE EXPENSE to maintain a physical IT infrastructure, the thought of replacing server rooms and haphazardly configured appliances with cloud services is simply too hard for many companies to resist. But rushing into the cloud without a security strategy is a recipe for risk.

According to the survey, 43 percent of respondents are using cloud services such as software as a service or infrastructure as a service. Even more are investing in the virtualization technology that helps to enable cloud computing. Sixty-seven percent of respondents say they now use server, storage and other forms of IT asset virtualization. Among them, 48 percent actually believe their information security has improved, while 42 percent say their security is at about the same level. Only 10 percent say virtualization has created more security holes.

Security may well have improved for some, but experts like Chris Hoff, director of cloud and virtualization solutions at Cisco Systems, believe that both consumers and providers need to ensure they understand the risks associated with the technical, operational and organizational changes these technologies bring to bear.

"When you look at how people think of virtualization and what it means, the definition of virtualization is either very narrow—that it's about server consolidation, virtualizing your applications and operating systems, and consolidating everything down to fewer physical boxes—or it's about any number of other elements: client-side desktops, storage, networks, security," he says. "Then you add to the confusion with the concept of cloud computing, which is being pushed by Microsoft and a number of smaller, emerging companies. You're left scratching your head wondering what this means to you as a company. How does it impact your infrastructure?"

Fortunately, there's some evidence of companies proceeding with caution.

One example is Atmos Energy, which is using Salesforce.com to speed its response time to customers and help the marketing department manage a growing pool of clients, according to CIO Rich Gius.

The endeavor is successful thus far, so Gius is investigating the viability of running company e-mail in the cloud. "It would help us address the growing challenge where e-mail-enabled mobile devices like BlackBerrys are proliferating widely among the workforce," he says. But he's not ready to take such a big step because the risks, including security, remain hard to pin down. One example of the disruption that cloud-dependent companies can experience came in May, when search giant Google—whose content accounts for 5 percent of all Internet traffic—suffered a massive outage. When it went down, many companies that have come to rely on its cloud-based business applications (such as e-mail) were dead in the water.

The outage wasn't caused by hackers, but there are signs that cybercriminals are exploring ways to exploit the cloud for malicious purposes. On the heels of the outage, attackers added insult to injury by flooding Google search results with malicious links, prompting the U.S. Computer Emergency Response Team (US-CERT) to issue a warning about potential dangers to cloud-based

Data Dangers

Attacks on data have increased faster than any other security exploit. The top target: databases.

HOW ATTACKERS GET YOUR DATA

57%	Databases
46%	File-sharing applications
39%	Laptops
23%	Removable media
16%	Backup tapes

NOTE: MULTIPLE RESPONSES ALLOWED

Illustration by iStockphoto.com

service sites.

The attack poisoned several thousand legitimate websites by exploiting known flaws in Adobe software to install a malicious program on victims' machines, US-CERT says. The program would then steal FTP login credentials from victims and use the information to spread itself further. It also hijacked the victim's browser, replacing Google search results with links chosen by the attackers. Although the victimized sites were not specifically those offering cloud-based services, similar schemes could be directed at cloud services providers.

IT organizations often make an attacker's job easier by configuring physical and cloud-based IT assets so poorly that easy-to-find-and-exploit flaws are left behind. Asked about the potential vulnerabilities in their virtualized environments, 36 percent cited misconfiguration and poor implementation, and 51 percent cited a lack of adequately trained IT staff (whose lack of knowledge leads to configuration glitches). In fact, 22 percent of respondents cited inadequate training, along with insufficient auditing (to uncover vulnerabilities) to be the greatest security risk to their company's cloud computing strategy.

It's this awareness that makes Atmos Energy's Gius proceed with caution. "We have no CSO. If we were a financial services firm, it might be a different story, or if we had a huge head count," Gius says. "But we are a small-to-medium-sized company, and the staff limitations make these kinds of implementations more difficult."

Even with the right resources, security in the cloud is a matter of managing a variety of risks across multiple platforms. There's no single cloud. Rather, "there are many clouds, they're not federated, they don't natively interoperate at the application layer and they're all mostly proprietary in their platform and operation," Hoff says. "The notion that we're all running out to put our content and apps in some common [and secure] repository on someone else's infrastructure is unrealistic."

Lobel, with PricewaterhouseCoopers, says perfect security is not possible. "You have to actively focus on the security controls while you are leaping to these services," he says. It's difficult for companies to turn back once they have let their data and applications loose because they are often quick to rid themselves of the hardware and skills they would need to bring the services back in-house.

"If you dive down a well without a rope, you may find the water you wanted, but you're not going to get out of the well without the rope," he says. "What if you have a breach and you need to leave the cloud? Can you get out if you have to?"

Security Budgets Hold Steady

More companies are increasing spending than cutting it

DIRECTION OF SPENDING

38%	Increase
25%	Stay the same
12%	Decrease
24%	Don't know

NOTE: NUMBERS MAY NOT ADD TO 100% DUE TO ROUNDING

TREND #3

Insourcing Security Management

A FEW YEARS ago, technology analysts were predicting unlimited growth for managed security service providers (MSSPs). Many companies then viewed security as a foreign concept, but laws such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act (affecting financial services) were forcing them to address intrusion defense, patch management, encryption and log management.

Convinced they couldn't do it on their own, companies chose outsourcers to do it for them. Gartner estimated the MSSP market in North America alone would reach $900 million in 2004 and that it would grow another 18 percent by 2008.

Then came the economic tsunami, which appears to have cast a shadow over outsourcing plans even though security budgets are holding steady. Although 31 percent of respondents this year are relying on outsiders to help them manage day-to-day security functions, only 18 percent said they plan to make security outsourcing a priority in the next 12 months.

When it comes to specific functions, the shift has already begun. Last year, 30 percent of respondents said they were outsourcing management of application firewalls, compared to 16 percent today. Respondents cited similar reductions in outsourcing of network and end-user firewalls. Companies have also cut back on outsourcing encryption management and patch management.

At the same time, more companies are spending money on these and other security functions. Sixty-nine percent said they're budgeting for application firewalls, up slightly compared to the past two years. Meanwhile, more than half of respondents said they are investing in encryption for laptops and other computing devices.

The results surprise Lobel of PricewaterhouseCoopers. "When you think about it logically, some IT organizations have the resources and maturity to manage their operating systems and patches, but many don't," he observes. "Hopefully, the numbers simply mean IT shops have grown more mature in their security understanding."

How Cybercrime Costs You

Losses from incidents average $833,000

THE BUSINESS IMPACT OF SECURITY BREACHES

42%	Financial loss
30%	Brand or reputation compromised
29%	Intellectual property theft
20%	Home page altered or defaced
17%	Fraud

NOTE: MULTIPLE RESPONSES ALLOWED

Lopez, formerly from MSC Software and Stamps.com, observed a stark trend

toward less outsourcing while at MSC (he left the company earlier this year).

"The company was doing less and less outsourcing. It was mostly due to the economic conditions more than anything else," he says. "They were certainly looking to see where cost could be reduced or eliminated. I also hear from a few of my friends in other companies that the trend is toward doing more with internal staff."

Peter Hillier, director of IT security for CMA Holdings in Ottawa, believes there are three things driving the move toward more in-house security:

1. Organizations have become more adept at do-it-yourself security since first outsourcing, though, Hillier says, "they should have done that prior to outsourcing security the first time."

2. SIM/SIEM growth has been as good for the insourcer as it is for the outsourcer. "If you can do more with less, then why pay someone else to do it?" Hiller asks.

3. Economy is a driver, as others have noted.

Charles Beard, SVP and chief information officer for Science Applications International Corp. (SAIC), says that no matter what drives security spending decisions, companies should understand their specific security strategies and where managed security providers can offer unique value. Smart business executives understand that they must maintain control of the big picture at all times, even if a third party is managing many of the levers. Keeping an eye on security service providers and the risks they are encountering is essential. "CIOs and security officers may outsource certain functions to various degrees, but they should never outsource their responsibility," Beard advises.

What Drives Security

Business continuity and the economy lead the reasons for investing

41%	Business continuity/disaster recovery
39%	Economic downturn
38%	Internal compliance
37%	Regulatory compliance
30%	Change

NOTE: MULTIPLE RESPONSES ALLOWED

TREND # 4

A New Corporate Commitment

COMPANIES MAY STILL struggle with the quality of their data security, but the response to this year's survey suggests their executive peers have agreed, finally, that security can't be ignored.

Companies' budget plans tell part of the story. Not only are more companies investing in security technologies, but overall security investments are largely intact, despite the economy.

Twelve percent of respondents expect their security spending to decline in the next 12 months. But 63 percent say their budgets will hold steady or increase (although fewer foresee increases than did last year).

For starters, more companies are hiring CSOs or chief information security officers. Eighty-five percent of respondents said their companies now have a security executive, up from 56 percent last year and 43 percent in 2006. Just under one-third of security chiefs report to CIOs, 35 percent to CEOs and 28 percent to boards of directors.

Two factors are influencing companies to maintain security as a corporate priority: Seventy-six percent say the increased risk environment has elevated the importance of cybersecurity among the top brass, while 77 percent said the increasingly tangled web of regulations and industry standards has added to the sense of urgency.

Respondents were asked how important various security strategies had become in the context of harsher economic realities. Seventy percent cited the growing importance of data protection while 68 percent cited the need to strengthen the company's governance, risk and compliance programs.

Notes Mauricio Angée, senior manager of IT security and compliance, and CSO at Universal Orlando: "For segregation of duty purposes, it's interesting to see how companies are being asked—by compliance auditors, qualified security assessors and through legislation—to hire IT security managers with a much-more-defined set of roles and responsibilities." Such roles include setting the company's security policy, making the security budget pitch (instead of the CIO) and delegating responsibility among lower-level IT security administrators and engineers.

None of these developments, however, make a focus on information security a sure bet in the eyes of IT leaders. Just because companies feel they have to spend money on security doesn't mean executives view it as an essential, even beneficial business process instead of a pain-in-the-neck task being forced upon them.

Angée says security leaders still have to fight hard for every penny. Meanwhile, security execs don't have the same decision-making power as other C-level leaders in every company, says PricewaterhouseCoopers' Lobel. CIOs can bring in a CSO or CISO without a strategy and budget for that person to work with, and end up achieving nothing. If something goes wrong, he concludes, "all you'll have is somebody to blame and fire." ■

Reach Senior Editor Bill Brenner at bbrenner@cxo.com.

How We Got the Numbers

The seventh-annual "Global State of Information Security" survey—a worldwide study by *CIO*, *CSO* and PricewaterhouseCoopers—was conducted online from April 20, 2009, through June 23, 2009. *CIO* and *CSO* print and online customers, and clients of PricewaterhouseCoopers from around the globe, were invited to take the survey. Results are based on responses from 7,276 security and information technology professionals from more than 100 countries. Thirty-two percent of respondents were from North America, followed by Asia (27 percent), Europe (26 percent), South America (14 percent) and the Middle East and South Africa (2 percent). The margin of error for this survey is +/- 1 percent.

-Carolyn Johnson, research manager

At the *Ready*

Chemical giant Dow brings free hazmat-spill education and awareness to emergency responders

By Joan Goodchild

How prepared are emergency responders for dealing with a chemical spill that could have serious health and environmental implications? The answer to that varies widely depending on the size of the community and the budget of the emergency departments. That's where a program called Transcaer comes in.

Transcaer, which stands for Transportation Community Awareness and Emergency Response, is a national outreach effort that brings chemical and transportation industry experts into local communities to provide free transportation and chemical safety training to emergency personnel. The Dow Chemical Company has been running the program for 23 years and has seen it expand significantly in recent years. Dow recently partnered with Union Pacific to bring training to all communities along the companies' shared routes by 2012 and expects more growth by bringing the program to communities in Mexico and Canada.

The program brings emergency responders from small communities into hands-on training sessions that focus on railroad equipment training, hazardous material handling and emergency response drills. Tim Scott, chief security officer and director of emergency services and security for Dow, gave *CSO* an overview of the program and its mission.

The Transcaer program is free training for responders in communities that might not be able to afford it otherwise. Tell us more about that.

The program is really designed to get out to the small communities. The people that really benefit from this are the small cities that don't have the big budgets to send responders to a course like this. Typically it would be a thousand dollars a person to go to a course like this. We do a whistle stop tour and we stop and do a one-day course in these communities. We go from small city to small city because that is the audience we are looking to touch.

This program has been around for 23 years. What's changed since its inception?

Since 2001, a lot has changed. A lot more people have become engaged in it. There is a lot more community involvement, a lot more government involvement. The program started with two companies out doing their own program and working with it with their local communities. But it has now expanded to dozens of companies across the nation. Various industry associations are involved now and a lot of government agencies are involved. So it has grown from a few people sitting in a conference room to hundreds of people working on this process across the nation. Through the years, we have helped train and raise the awareness of literally thousands of responders.

Give us some details about the training responders receive.

We have training cars that actually go to the scene for the training. We have a classroom car where you actually sit in and some classroom-type training. But the strong part about it is we have real cars that responders may see out on a scene. They can get up on top of cars, look at the configuration of the cars. We have cars that come apart and you can open them up to see what they look like inside. You can actually touch the valves and change the valves and see how the valves work. You can suit up in the equipment you are going to have to wear if

Photos courtesy Dow Chemical

you respond to a scene. It's really a hands-on training so when they arrive on a scene, it's not the first time that they have ever seen the situation or the rail cars, or the equipment they are going to have to use.

What kind of scenario do you lay out for responders who are training?
Any kind of chemical spill: Derailment of a rail car, for instance. Or a truck overturns carrying chemicals.

The training starts off with recognition of the problem. There are some problems where you just back off and call in people that respond to these kinds of emergencies all the time. So the first step is to recognize: What is the situation? What is the chemical involved? Do you have the right experience to address that issue? Do you have the right equipment? If the answer is yes, you can go in and start to do the initial assessment of the emergency and call in the right people to help as needed. It's really about safety for the responders so they don't rush into something and get themselves injured.

How do you train responders to move or handle hazardous materials?
With both hands-on training about specific types of chemicals and classroom training to understand the different characteristics of the chemicals and their different hazards.

Most major cities have very experienced hazmat response teams. If you look at cities like Houston, Chicago or New York, they have well-trained teams. As you get into smaller communities, especially communities that have volunteers, such as volunteer fire departments, they do a very good job at what they do, but hazmat response is not something they do every day. We give them the recognition class so they know how to recognize, when to pass on information, when they need to evacuate the area to protect the community.

Who are the folks that generally take part in these sessions?
We do a few classes. The police department is usually first on the scene. They get the awareness and recognition class. But their role description is typically to secure the scene. They don't respond to fix the event. They respond to secure the area so the community doesn't wander in and get themselves hurt. So it's awareness training we give to police.

The actual responders—from the fire department or contract companies that are hazmat responders—we give the hands-on training of how to deal with specific chemicals, railcars and those areas.

What kinds of chemicals would commonly be involved in an emergency scenario?
Any you can think of. Some of the major ones that you hear about are chlorine and oxidizers. You hear about explosives. So everyone has a different kind of response. But most hazmat chemicals that are being transported around the country are very critical to various products and things we use every day.

Does training get as detailed as being able to tell the difference between one chemical and another?
They are trained to know the class of chemical. All railcars are marked with specific Department of Transportation markings so you know if you are dealing with a corrosive material or an explosive material, and you can look at the car and tell if it's full or empty.

How serious can these spills be? What kind of danger might a community face?
There are both health concerns and environmental concerns; those are the two big issues you are trying to eliminate. For example: Look out on the highway and you'll see the number of trucks that are carrying gasoline. That can be a very hazardous material in the wrong situation. We try to look at things that we know are truly hazardous materials.

Another thing to keep in mind, from an industry perspective, is if a truck goes around the corner and spills milk in someone's front yard, they don't know what that is. So we try to give them the right contact numbers so someone can get out there and handle that situation appropriately.

Have there been instances when communities you've trained have had to put this education into practice and have told you the training really helped?
We've got some feedback like that over the years. The good news is these spills are not in the news, which means they are being handled appropriately by responders. Between either awareness or the actual response, you don't have any injuries and that's what we want. ■

You can reach Senior Editor Joan Goodchild at jgoodchild@cxo.com.

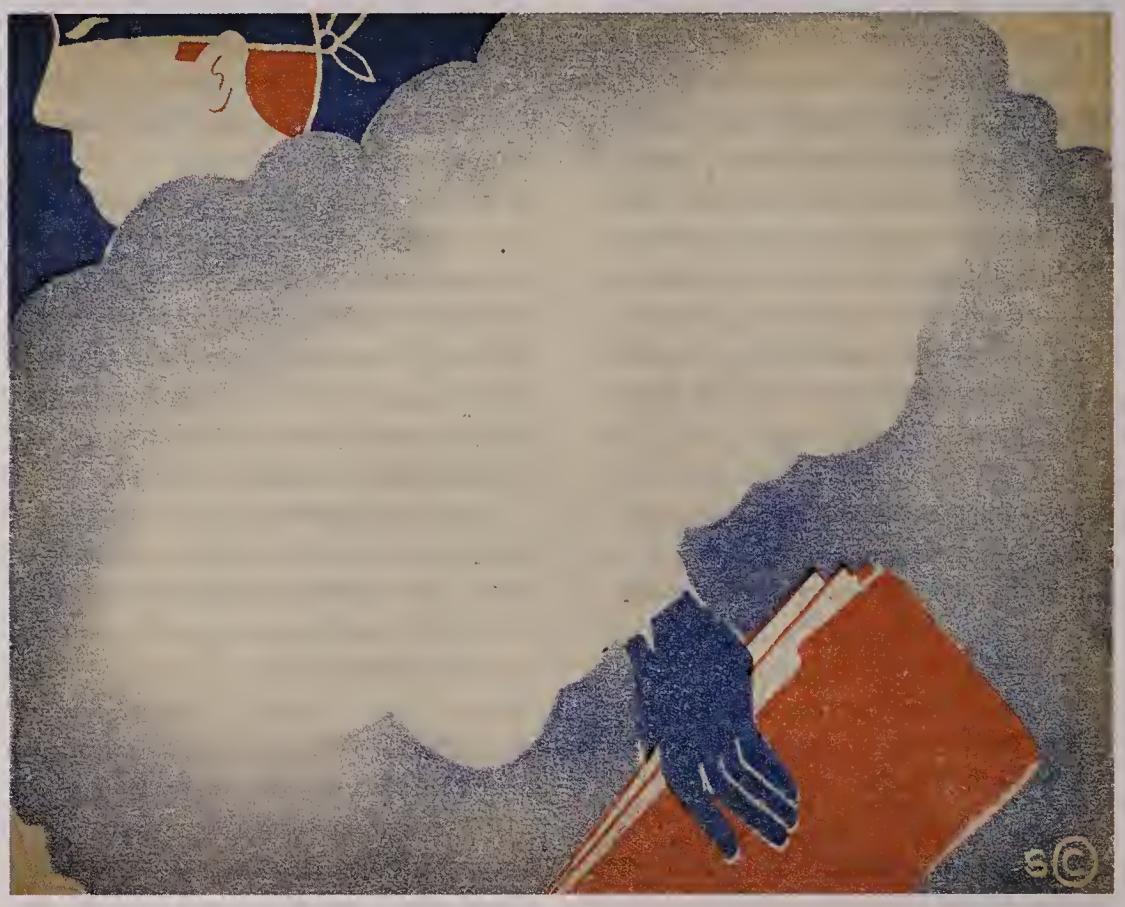
From left: 1) Dow's traveling Transcaer program brings chemical and transportation industry experts into small communities for training that focuses on railroad equipment and hazardous material handling; 2–3) The program gives emergency responders hands-on training and features rail cars where responders learn; 4) Training cars come apart and allow students touch valves; 5) Without Transcaer, rural-area community responders who attend sessions might otherwise not receive this kind of education, says Dow.

[INDUSTRY VIEW]

By Ira Winkler

The Real Problems With Cloud Computing

Google may well protect servers better than you do. But your job is to protect information—not just servers.



The recent Twitter breach, where a French hacker compromised internal Twitter documents by accessing the account of an administrative assistant, among others, was essentially an attack on Google Docs. The reason is that Twitter outsourced its infrastructure by contracting with Google, and the accounts in question were on Google's infrastructure.

News reports of the incident questioned the security of Google Apps and cloud security in general. Google claimed that its security was better and less expensive than the security that companies could provide for themselves. At the same time, people (including me) continued to argue that exposed information is exposed information. This position is based on the idea that companies want to protect their information and not the computers. This can be extremely confusing for CSOs trying to decide whether or not to implement cloud computing. This issue is at the forefront, especially given Los Angeles County's stated intention to migrate to Google Apps.

Let's first acknowledge that Google Apps was not specifically "hacked" in the traditional sense of the word during the Twitter incident. A hacker did not break into Google computers through some technical vulnerability in the Google infrastructure.

A hacker found a personal e-mail account for the administrative assistant previously mentioned. Similar to the Sarah Palin Yahoo account hack, the hacker researched social networking sites to find the answer to the "secret question" required to reset the account's password. In going through the e-mails in the account, the hacker apparently found the password used by the administrative assistant on other sites, and correctly assumed that the person used that password on his Twitter corporate account at Google Apps.

This gave the hacker access to e-mails and files. Other information available to the account also allowed the attacker to compromise the Twitter corporate accounts of other employees.

While the initial reaction would be to blame the guessing of the security questions on the freemail account, as well as the reuse of the password, that is akin to saying people drown because of water. Clearly, there are many other vulnerabilities in cloud computing implementations that enabled the compromise of the accounts on Google Apps.

For example, the fact is Google Apps allowed anyone in the world to attempt to log in to any account at Twitter. In this case, the account holder was in the San Francisco area and the hacker logged in from France. If the accounts were maintained internally, Twitter would have had the ability to deny remote access. Similarly, if misuse and abuse detection tools had been used, even allowed accesses would have been flagged given the location and the scope of the data access. There are also data leak prevention (DLP) tools that could have been in place.

Google Apps doesn't provide for add-on security tools, such as those mentioned above. It does provide for SAML 2.0 authentication integration. However, that is a footnote, and organizations that are using Google Apps because they don't want to maintain the internal technical staff

Illustration by Sophie Casson

required to run office applications are not likely to maintain staff to manage a SAML-compliant tool, which can be complicated. Using an automobile analogy, it is like saying you will bring your car to a repair shop for everything, even simple oil changes, except for problems with the ignition system, which you agree to maintain entirely on your own.

There is a great deal of truth to the contention that Google can maintain the security of systems better than individual companies can. This specifically involves server security, not data security. For example, hackers target vulnerable operating systems that don't have properly applied patches. While I may be critical of some aspects of Google Apps security, I firmly believe that Google is significantly more likely to maintain the security of individual systems than user companies would be.

Google also implements sharding, which means that an individual file could be divided among hundreds of systems, in theory. This way, if someone actually does break into a server, he isn't likely to get a useful amount of information out of individual documents.

However, the fact is that attackers want your information, and they will get it however they have to. For example, the recent Heartland hacks resulted from an SQL injection that targeted the database applications, not servers. While Google Apps may better maintain fundamental security of its office applications, that again does not help with the access and sniffing potential.

Cloud computing puts your data outside of your organization. Also when you use a cloud computing service, you are limiting yourself to the amount of advanced security tools that you can put on the system. I already gave the examples of DLP and misuse and abuse detection, which are not available to Google Apps users. Likewise, you cannot limit the access to only internal staff. There are many other security tools that cannot be put in place in cloud environments, unless the cloud environment is specifically designed for them.

There are also other issues to consider. You have little control over how much audit information is collected. For example, you likely do not have access to failed login attempts, so you cannot proactively look for attack reconnaissance. Likewise, while you may maintain ownership of your data, you do not likely own all of the access log data. That potentially creates legal problems. For example, if someone does illicitly access your information, you might need to get a court order to see where he is located. If, however, you maintained your data internally, you would have instant access to all of this information.

I don't have enough space to bring up all potential limitations of cloud computing security. However, I intend to get you thinking about what you need to consider.

Let's face it: The $50-per-user annual fee for Google Apps is very attractive from a financial perspective. I also believe that CSOs should make decisions not from a security perspective, but from a risk perspective. Risk acknowledges that you have to make decisions that balance potential losses against potential cost savings.

If you wouldn't normally implement any additional security controls, like DLP or intrusion detection, you might as well use a cloud computing solution like Google Apps. Google would be much more likely to implement basic security controls better than you would.

However, if your organization has a great deal of intellectual property, and you believe that your data is valuable and intend to implement more than basic security measures, you probably need to maintain your own data infrastructure. You can, however, review cloud computing providers and see if they allow for the implementation of the security countermeasures you believe are necessary. A significant number of software vendors are beginning to offer cloud security products. The better cloud computing providers should be integrating these tools.

My perception of the Twitter hack is that Twitter is a company where money is not a driving force in infrastructure decisions. While it does plan for rapid growth, and Google Apps does allow for such growth, it is my belief that Twitter should implement more than basic security measures. After all, it eventually wants to move into the corporate market, and if it can't protect its own data, how can other companies trust Twitter?

Los Angeles County has different circumstances. While it clearly has more than enough value to justify maintaining its infrastructure internally, it seems like there is a major financial problem that might prevent it from doing so.

The $50-per-user annual fee for Google Apps is very attractive from a financial perspective. I also believe that CSOs should make decisions not from a security perspective, but from a **risk** perspective.

Unfortunately, given all of the regular abuse we see of government databases by authorized users, the county would be taking an unacceptable risk. The recent convictions of U.S. State Department employees for looking at celebrity travel records demonstrates the abuse that can only be detected when an organization has the ability to regularly review audit logs. Los Angeles County probably has a good deal of celebrity information, and people at various organizations have been accused of accessing medical information of celebrities. For example, the Octomom's medical records were leaked, as were those of Britney Spears and countless other celebrities. Without the ability to provide for automated misuse and abuse detection, Los Angeles County will miss a wide variety of criminal activities.

So while a cloud computing provider will likely better secure the servers, it isn't clear that they can secure information better than you can. The acronym CISO stands for chief information security officer, not chief computer security officer. That should give you an idea as to what your priorities should be. ■

Ira Winkler is President of Information Security Advisors Group.

[CSO VIEW]

By Ariel Silverstone

Where Defense in Depth Falls Short

Hearing about defense-in-depth can conjure up images of clutter. Ariel Silverstone says he's stumbled upon an example of a better way.

Defense in depth is arguably the most time-tested principle in security and applies to physical security as well as online. It builds on the concept of a hardened core where companies place their crown jewels. The core is then surrounded by castle walls and moats.

It's a great concept, but comes at a price. Just as the area covered is wider from layer to layer, so is the cost associated with protecting against more plentiful and less specific threats. A firewall typically acts as the last line of defense on the enterprise perimeter and has to protect against a variety of threats, while a server-room door only has to be concerned with physical access.

Another flaw in the design is that it's difficult to implement via the three basic tenets of security: confidentiality, integrity and availability. Why? Because most forms of defense create increasing confidentiality but make integrity more difficult to implement and manage. Any increase in defense, of course, makes the concept of availability that much harder to provide to the users.

Many of us resign ourselves to the proverbial "this is reality" and define our demarcation line as a physical device such as a router, an access point, a firewall or a Web server. There are potentially two things wrong with this:

- We are basically saying "we are a target just waiting to be attacked."
- We allow most barbarians (in the form of rogue traffic, networks and devices) to hit our gates.

If we continue to do so, we will have approached a mathematical certainty of being hacked, or at least of being hit with a denial-of-service exploit. Not only is the problem big enough to cause some to lose sleep, but imagine what happens when we move to a cloud topology. There, we have nothing but moats and walls and front doors. These front doors can be any browser, on any device, anywhere in the world. How do you protect yourself against that? Like any solution that might involve our entire user set, which may include Internet users rather than pure corporate users, any solution must be:

1. Easy to teach;

2. Easy to implement;

3. Applicable to the widest range of platforms possible;

4. Have a small delivery and storage footprint;

5. Easy to manage and maintain.

Knowing how rapidly threats evolve "in the wild," I also want a tool that does not go the normal route of blacklisting. I am more and more convinced that we need tools that no longer compare bad signatures or behavior to a database (which is how most antivirus and firewalls, for example, act) and we need to go the whitelist route. I want a tool that will be controlled by me and allow me to choose which domains can be accessed and under what (time or other) conditions can such an access occur.

To make matters even more interesting, I want control over certain user functions. For example, I would like some files to be able to be read and written, but not printed. Or that I be able to control launching certain tools, such as IM or browsers from within the session.

Finally, I want a bullet-proof audit trail. Until now, I did not see any solution to this quandary. Other than awareness and training, there was not a whole lot that could be done. Thanks to my friend Andreas Wuchner, the CISO of Novartis, I ran into a newly launched company called Quaresso. Started by a group of smart people with backgrounds in networking and security, in "Protect OnQ" they created both a new product and a service.

Working together, these allow us to do a few things: Select who will be allowed to knock on our doors and with what; select not only which browser is allowed to knock at your door, but also to choose what (and what NOT) that browser is allowed to contain—add-ins, plug-ins, encryption settings, printing ability (or not), security zone setting, etc. This effectively extends the defense in depth to the actual browser session!

Due to the implementation of the "armored" browser, data can no longer leak from it to the rest of the operating system. All passwords and personal information typed into a protected browser session remain confidential and unrecordable. I know I will sleep better. ■

Ariel Silverstone is a veteran of the Israeli Defense Forces with experience in physical and information security.

Illustration by Matthew Daley

CALL FOR ENTRIES

CSO Awards:

Recognizing Excellence in Security

CSO COMPASS AWARD

CSO NEXT AWARD

Nominations Open Until December 22, 2009!

CSO is proud to honor individuals that have advanced the security profession as well as rising stars within the industry.

Nominate a colleague—or yourself—to receive the CSO Compass Award or the CSO Next Award.

CSO Compass and Next Awards will be presented at the **2010 CSO Perspectives Conference** April 5-7, 2010 at the Hyatt Regency Santa Clara. Honorees—and their contributions to the security profession—will be featured on CSOonline.com and in the April issue of *CSO*.

To learn more about the awards and submit a nomination visit:
www.CSOonline.com/cso-awards/

Presented by:

CSO
BUSINESS RISK LEADERSHIP

[DEBRIEFING]

That's (Not) Hot

Google Trends shows which of two or three terms are used more frequently in Web searches. The gap between security terms and popular terms is wide indeed—unless you get a little creative in what you compare.

Graphs indicate total volume of Web searches for each specific term as of mid-October

DEMO people's choice

DEMO DRIVES INNOVATION

Enterprise Winner:

Liaise
turn words into action

Liaise, Inc. automates the capture and management of KeyPoints (tasks, issues, dates and priorities) buried inside emails, IMs and other communications. As you type, Liaise intelligently and automatically captures KeyPoints in your messages, and provides summaries, calendar integration and reports.

Consumer Winner:

EMO Emo Labs
Listen more™

EMO Labs, Inc. has changed the way you experience multimedia content with invisible, zero-footprint speaker systems. Imagine a TV with great stereo sound coming directly from the display panel, unifying audio and video for a more natural, realistic and compelling presentation.

Watch their Award-Winning Product Launches at:
www.demo.com/demopcwinners

DEMO continues to deliver the best innovation at DEMOspring 2010.
For complete information and to register, go to **www.demo.com**

BECAUSE PASSWORDS JUST AREN'T ENOUGH

Two-Factor Authentication

1. User enters username and password.
2. Instantly, user receives a call, simply answers and presses # (or a PIN) to complete the login.

Get the strong two-factor security you need to protect against today's sophisticated threats without the hassle and cost of yesterday's technology.

- Easy to Setup, Manage, and Use
- Strong Out-of-Band Authentication
- Rapid Regulatory Compliance
- Far Less Expensive Than Tokens

"Even if a hacker has your password, your account remains secure." – New York Times

PhoneFactor

www.phonefactor.com | 1.877.NoToken